A4

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06K 9/00 — A1

(11) International Publication Number: WO 91/06920

(43) International Publication Date: 16 May 1991 (16.05.91)

(21) International Application Number: PCT/US90/06172

(22) International Filing Date: 31 October 1990 (31.10.90)

(30) Priority data:
430,421 2 November 1989 (02.11.89) US

(71) Applicant: TMS, INCORPORATED [US/US]; 1060 Tiogue Avenue, Coventry, RI 02816 (US).

(72) Inventors: GAGNE, Patricia, C. ; PUTERKO, Carol, M. ; 7 Juniper Hill Drive, Coventry, RI 02816 (US).

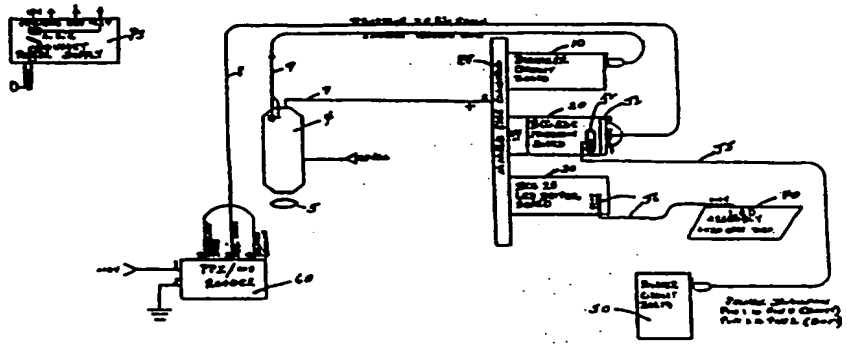
(74) Agent: DEL GIUDICE, Paul, V.; 2001 Jefferson Davis Highway, 1203 Crystal Plaza Building, Arlington, VA 22202-0286 (US).

(81) Designated States: AT (European patent), AU, BE (European patent), BR, CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent), SU.

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: NON-MINUTIAE AUTOMATIC FINGERPRINT IDENTIFICATION SYSTEM AND METHODS

(57) Abstract



The invention relates to a system and methods for verifying a person's identity, and pertains in particular to such a system and methods which utilize comparison of a fingerprint pattern for identification verification. The image of a fingerprint of a person to be identified is provided on an inkless means which when touched by finger of the person causes immediate development of an image of the fingerprint of the finger in a black and white appearance. This image of a fingerprint is video scanned (60) to produced image data which is digitized (10) to produce a non-minutiae digitized numerical identifier indicative of the fingerprint. A preferred method and system provides a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data which is recordable within the magnetic stripe of a credit card personal to a person, or may be recorded within the confines of a portable personnel identification means, or within a smart card, personal to a person. The non-minutiae digitized numerical identifier is provided by selectively analyzing different parts of a fingerprint and deriving from each part a byte numeric which is directly related to the ridge count computed for that part. Prior to performing the "digitizing" method, a fingerprint identity window is defined as the area of analysis. The present invention also discloses inventive methods relating to "image sizing" and "image framing" which are performed upon the fingerprint image and whitespace digital data stored in memory, prior to defining a fingerprint identity window. Various applications of the invention methods and system are disclosed herein.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MR	Mauritania
BE	Belgium	GA	Gabon	MW	Malawi
BF	Burkina Faso	GB	United Kingdom	NL	Netherlands
BG	Bulgaria	GR	Greece	NO	Norway
BJ	Benin	HU	Hungary	PL	Poland
BR	Brazil	IT	Italy	RO	Romania
CA	Canada	JP	Japan	SD	Sudan
CF	Central African Republic	KP	Democratic People's Republic of Korea	SE	Sweden
CG	Congo			SN	Senegal
CH	Switzerland	KR	Republic of Korea	SU	Soviet Union
CI	Côte d'Ivoire	LI	Liechtenstein	TD	Chad
CM	Cameroon	LK	Sri Lanka	TG	Togo
DE	Germany	LU	Luxembourg	US	United States of America
DK	Denmark	MC	Monaco		

NON-MINUTIAE AUTOMATIC FINGERPRINT IDENTIFICATION SYSTEM AND METHODS

BACKGROUND OF THE INVENTION

The invention system and related methods are directed to the automatic identification of fingerprints by video scanning and digitizing analysis of the scanned fingerprint, and to the general field of verification of the identity of a person to be identified, such verification being accomplished by comparing a non-minutiae digitized numeric identifier indicative of a fingerprint of a person to be identified with a numeric identifier recorded within the confines of a portable personnel identification means, personal to the person to be identified, which identification means can be of numerous kinds such as a retail credit card, a smart card, or others as set forth hereinafter. The numeric identifier of such portable personnel identification means is previously derived in accordance with the teachings of the present invention and then recorded within the identification means to enable identity verification, accomplished by comparison.

It is most desirable to have automatic means and methods for identifying human beings. Millions of individuals are checked on a daily basis by cumbersome and unreliable methods in banks, retail stores, classified areas, security environments, and by law enforcement officials. The problem of verifying the identity of an individual to a personnel identification card means held and offered as proof of identification by such individual, is one of the most common faced in the everyday duties of commerce, industry and government. Present day fingerprint verification methods are too time consuming and cumbersome to be expediently implemented into the civilian and military affairs of today's society. What is clearly needed is a means of, and methods for, providing automatic, rapid and positive verification of a person's identification.

The system invention, and the inventive methods utilized therein and related thereto, satisfy this long felt need for methods and means for providing automatic verifiable identification of an individual submitting him or herself for identification for the purpose of: retail credit card purchases, authorized entry, check cashing, obtaining a driver's license, showing proof of age via a driver's license, verification of the identity of a holder of a passport, etc.

A further great need is the development of such a system and methods for providing a verifiable fingerprint identifier which is most applicable to and recordable within a magnetic-stripe of a portable personnel identification card means, such as a magnetic stripe of a credit card. The least number of bytes within a verifiable fingerprint identifier, known to the inventors of the present invention, is a 400 byte numeric identifier developed by FINGERMATRIX. This known development is not at all applicable to a portable personnel identification card of the magnetic-stripe type for reasons well known to those skilled in this art.

The presently disclosed system invention and the inventive methods thereof fully satisfy this further need by providing a verifiable non-minutiae fingerprint identifier having but 24 bytes of fingerprint identification data which affords recordability to magnetic-stripe identification cards.

The invention includes the actual taking of an individual's fingerprint via an inkless means each time an identification is to be made. The print can be taken of any digit of a person, i.e. index finger or thumb or toe, and the image of a digitprint is video scanned to produce image data which is digitized in accordance with the teachings of the invention to produce a non-minutiae digitized numerical identifier indicative of the digit print image, and this digitized numerical identifier is compared with a numerical identifier read from an

identification card means identifying the person to be identified, to verify the identity of that person.

Various other objects and advantages of the invention methods and system will be apparent from that set forth hereinafter, and some of the specific objectives of the invention are recited hereinbelow.

OBJECTS OF THE INVENTION

It is an object of the invention to provide a biometric means for comparing the fingerprint of an individual whereby a rapid and highly fraud-proof check may be made.

It is another object of the invention to make the fingerprint image expediently available for immediate analysis to render approval or disapproval of the identity of a given person from whom the fingerprint is taken.

It is a general objective of the invention to provide a system and related methods by which an individual fingerprint may be video-scanned and digitized in such a manner that the procedure produces a numeric identifier uniquely related to the pattern of the fingerprint, this identifier consisting of a specified number of digits or bytes to identify the fingerprint against an actual fingerprint of an individual at the time positive identification is required.

It is a specific object of the invention to provide a non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data, and in particular, a verifiable identifier having less than 100 bytes of fingerprint identification data for application to mag-stripe personnel identification cards, as exemplified by the provision disclosed herein of a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data.

It is yet another object of the invention to provide means by which a fingerprint image format may be positioned automatically in relation to the video scanning

means, in such a way that the position is predetermined and will be reestablished each time that a print format means is placed before the video scanner, thus insuring that a subsequent scanning operation will always produce consistent and reliable field of scan results.

It is still another object of the invention to provide means and methods for selectively analyzing a plurality of different fingerprint pattern parts of the stored fingerprint image data and computing a ridge count for each of the plurality of fingerprint pattern parts, and then compiling a data matrix comprised of a plurality of ridge counts computed for the plurality of fingerprint pattern parts to provide a non-minutiae digitized numerical identifier indicative of the image of a fingerprint of a person to be identified.

It is still another object of the invention to provide a predetermined sequence of selectively analyzing a plurality of different fingerprint pattern parts of the stored fingerprint image data, which fingerprint pattern parts exist within a fingerprint identity window defined by the invention.

It is yet still another object of the invention to provide a non-minutiae digitized numerical identifier indicative of an image of a fingerprint of a person to be identified, which is recordable within the magnetic stripe of a credit card personal to the person and therefore, the present invention facilitates the use of a credit card as a verifiable identification card for entitling the user to certain services such as charged purchases and check cashing.

It is even a further object of the invention to provide a fingerprint identification system and inventive methods utilized therein, which can be completely software controlled and automated to eliminate the possibility of human error, to increase the reliability of the identification being made and to eliminate any constant supervision as usually required with conventional

identification procedures. The invention, by utilizing an unchanging characteristic of an individual for making an identification, is not subject to obsolescence and at the same time may be constructed at various levels of sophistication depending on the degree of security of reliability which is desired. The system can be made an integral part of other systems in which information about individuals is taken and recorded and the system can be so constructed with controls that provide for immediate revocation of the privileges of benefits given any individual identified in the system.

It is also another object of the invention to provide a method for the automatic non-minutiae identification of a fingerprint of a person to be identified which includes a method for determining the location of the fingerprint image data stored in a memory means with the whitespace data produced by scanning an image of a fingerprint, and to define a fingerprint or digitprint identity window so as to define a predetermined "area of analysis", which area is defined depending on the specific needs of the end-user application, and with respect to a predetermined "window-size", to enable defining the dimensional area of the fingerprint identity window.

The foregoing and other objects, features and advantages of the invention will be apparent from the following more detailed description of preferred embodiments and methods of the invention, as illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1A shows an inkless framed format having produced thereon an image of a fingerprint.

FIG. 1B shows the inkless framed format holder means which is mounted on the face of the system housing.

FIG. 2 shows the predetermined position orientation of a video scanning camera and a 16 mm lens to the center of an inkless framed format positioned within the framed format holder means.

FIG. 3 shows a portable personnel identification card of the magnetic-stripe kind.

FIG. 4 is a flow diagram of the system manual and hardware flow of the present invention.

FIG. 5 is a flow diagram of the software process of fingerprint identification verification of the present invention.

FIGS. 6A and 6B is a combined flow chart diagram of the manual, firmware and software process flow of the present invention.

FIGS. 7A, 7B, 8A, 8B, 9A, 9B, 10A, and 10B jointly depict the Image Frame Sizing Routine of the invention, wherein the respective method steps are shown in two forms. FIGS. 7A, 8A, 9A, and 10A, illustrate the values computed in reference to a fingerprint image produced on an inkless framed format means; and FIGS. 7B, 8B, 9B and 10B provide illustrations of how the respective values are determined from the performance of their respective method steps which are performed on the digital fingerprint image and whitespace data stored in the memory means of the video digitizer, in accordance with the teachings of the present invention.

FIGS. 11A and 11B depict in a fashion similar to FIGS. 7 - 10, a method step of the Algorithm Data Generation Routine, wherein the inventive methods of defining a fingerprint identity window and determining the dimensional area of such window, are accomplished.

FIG. 12 illustrates the computation of count S1.

FIG. 13 illustrates the computation of count S2.

FIG. 14 illustrates the computation of count Yam.

FIG. 15 illustrates the computation of count Ybm.

FIG. 16 illustrates the computation of count Ya.

FIG. 17 illustrates the computation of count Yb.

FIG. 18 illustrates the computation of count Yc.

FIG. 19 illustrates the computation of count Xam.

FIG. 20 illustrates the computation of count Xbm.

FIG. 21 illustrates the computation of count Xa.

FIG. 22 illustrates the computation of count Xb.

FIG. 23 illustrates the computation of count Xc.

FIG. 24 depicts a block diagram of the system invention.

FIG. 25 illustrates the System Bus Pinout diagram for interconnection of the digitizer 10 to the MMZ8 edge connector Z8.

FIG. 26 illustrates the MMZ8 bus pin configuration interconnections of processor 20 and the Z8 edge connector via J4.

FIG. 26A illustrates the interconnections of LCD Driver 30 with Z8.

FIG. 27 illustrates a console serial connector J1 which is utilized to interconnect the PPI/MS Reader 60 with processor 20.

FIG. 28 illustrates the serial printer connector J2 which is utilized to interconnect the processor 20 with the printer 50.

FIG. 29 illustrates one embodiment of the system invention employed in application pertaining to personnel identity verification, which embodiment incorporates the use of PPI/MS Reader 60.

FIG. 30 illustrates a second embodiment of the system invention employed in an application pertaining to personnel identity verification, which embodiment incorporates the use of a smart card identification means.

FIG. 31 illustrates a third embodiment of the system invention employed in an application pertaining to check cashing-personnel identity verification of check payee, which embodiment incorporates the use of PPI/MS Reader 60 and printer means 50.

FIG. 32 illustrates the connection of printer 50 to the processor 20.

FIG. 33 is a flow diagram of a firmware/software control process of the present invention.

FIG. 34 is a flow diagram of a software process of the invention for card initialization.

DEFINITIONS

It is well known that fingerprints contain specific features, called minutiae, which are unique and allow identification of people by their fingerprints or even a toe print. By definition, a minutiae is either: (1) a bifurcation, which is the location where a given line forks into different lines; or (2) a ridge ending. Minutiae are usually recorded with three coordinates: two coordinates "x" and "y" for the position of the minutiae relative to a coordinate system: and one coordinate "a", which is an angle representing the average direction of the lines around the minutiae point.

In contrast, the present invention methods and system are "non-minutiae" based and either provide or utilize a non-minutiae digitized numerical identifier which is uniquely related to the pattern of a fingerprint it identifies. The non-minutiae digitized numerical identifier is provided by selectively analyzing different parts of a fingerprint and deriving from each part a byte numeric which is directly related to the ridge count computed for that part. This non-minutiae digitized numerical identifier can also be described as a "verification string".

The term "digitizing" is used herein to refer to the process by which the non-minutiae digitized numerical identifier is derived by the respective invention methods disclosed herewith; and, the term "digitized" is used herein to identify the non-minutiae numerical identifier derived by such process.

The "ridge counts" are computed by analyzing or examining selected horizontal and vertical and diagonal memory data lines of the fingerprint identity window

defined by the present invention, and counting the number of greylevel shifts from "white" (greylevels 13, 14 or 15) to "black" (greylevels 0 through 12).

The video digitizer of the system invention is the means employed for converting the video scanned fingerprint image data (FID) and whitespace data into digital data to generate within its memory a digitalized picture of that scanned by the video scanner, i.e. the inkless format providing an image of a fingerprint of a person to be identified; but, it is the software-controlled processor means of the invention which functions to selectively analyze the digital data to provide a digitized numerical identifier indicative of the fingerprint image.

The present invention discloses an inventive method step termed "image framing" wherein, prior to selectively analyzing different parts of the fingerprint image data and prior to defining a fingerprint identity window, the fingerprint image and whitespace digital data stored in an addressable memory means (RAM), located in the video digitizer, are framed to a predetermined dimension, and the location of the fingerprint image data stored in this memory means with whitespace data is determined by determining: (1) X-START and X-END values to indicate the start and the end of the fingerprint image data along the X-axis, and (2) Y-START and Y-END values to indicate the start and end of the fingerprint image data along the Y-axis. The "image framing" invention method also includes an "image frame sizing" step which essentially frames the digital fingerprint and whitespace image data contained in memory.

The "fingerprint identity window" defined by the present invention is the "area of analysis" defined within the fingerprint image data stored in memory. It is this fingerprint identity window which is selectively scanned and analyzed in accordance with the teachings of the present invention, to provide a non-minutiae digitized numerical identifier indicative of the fingerprint image

data of a fingerprint of a person to be identified. The "fingerprint identity window" is defined depending on the specific needs of the end-user application, and is set by determining a "window-size".

The purpose of the "verification string" is to provide a tailorable degree of certainty into the comparison of encoded data on i.e., the magnetic stripe of a credit card, or other article presented by an individual used as a personal identification means, and the individual's fingerprint image.

This "verification string" can be variable in size, depending on multiple factors. The invention affords the provision of a verification string (or digitized numerical identifier) which has less than 400 bytes of fingerprint identification data, or one having less than 100 bytes of FID as applicable to a magnetic stripe credit card or a smart card or other personal identification card means, or, in particular, an identifier having only 24 bytes of FID which as disclosed in a preferred method and embodiment of the present invention is uniquely applicable to the magnetic stripe of a credit card.

An "element" is a calculated value, generated by the end-user application.

A first factor is the size of the "window" in which image analysis is performed. The larger the window, the more verification data can be generated for comparison purposes. Since the "window" is variable depending on end-user applications, the size of the verification string can vary as well. Thus, it is reasonable to say that increasing the "window-size" used in verification string generation presents the opportunity to increase the number of elements which comprise the verification string.

A second factor is the formulas or calculations used to generate or calculate the verification string. The calculations performed to generate the verification string can vary from one end-user application to another. Any mathematical formula or statistical computation based on

ridge counts, whether individually or as a sum, can be used as an element in the verification string data matrix which is compiled.

Both of the above scenarios address the flexibility of the verification string size in designing end-user applications with varied degrees of verification confidence. Of course, different applications might have the same number of verification string elements, yet comprise of entirely different formulas used to generate that data. In other words, two end-user applications may comprise verification strings having a different total number of elements, and the applications may generate each element of its verification string differently.

Lastly, the positioning of each element within the verification string could be different from one application to another. For instance, one application might use Yc (Y Center Line Count) as a value for the seventh element of the verification string, as disclosed herein, and yet another application may use the same value in another element of its verification string.

DETAILED DESCRIPTION OF INVENTION METHODS

A preferred form of the present invention system and methods combinatively utilize an inkless media for the purpose of taking or providing an image of a fingerprint or digitprint. An image of such print is produced by placing a digit of the person to be identified within a 2" x 2" framed format 1 as shown in FIG. 1A, which contains a treated material which when touched by a finger, utilizing an inkless process, causes immediate development of an image of a fingerprint of such finger in a black and white appearance, to provide a good quality scannable image of a fingerprint. The use of this inkless means for taking a fingerprint of a person to be identified overcomes the disadvantages of conventional fingerprint taking techniques. Of course, it is within the scope of the present invention to be applicable to video scan a fingerprint image imprinted upon other media, or by other methods.

After the fingerprint has been taken, the inkless framed format 1 is placed within a format holder 3 which is mounted on the face plate of the system housing. The placement of the inkless framed format within the format holder 3 is illustrated in FIG. 1B.

FIG. 2 shows the predetermined position orientation of a video scanning camera 4 and a 16 mm lens 5 associated therewith, to the center of the inkless framed format when it is positioned within the format holder. The center 6 is the center of the inkless media 2 bearing the fingerprint image. A preferred predetermined distance of 2 1/2 inches is set between the center 6 and the face of lens 5.

Accordingly, this provides means by which a fingerprint may be positioned automatically in relation to a video scanning system, in such a way that the position is unique and will be reestablished each time that the framed format 1 is placed within the format holder and thus within the field of scan of the video scanner, to insure that any

subsequent scanning operation will always produce proper and desirable results. The use of the inkless fingerprint media for taking the person's fingerprint without requiring the direct application of ink to the person's finger, and under controlled conditions, affords that the person's print may be repeatedly produced with the same clarity and detail, thus facilitating an accurate comparison between prints.

After the fingerprint has been taken on the inkless means of the framed format, the framed format 1 is placed within the holder 3 with the fingerprint image facing the housing face plate and towards the field of view of the video scanner. It is to be noted that in an effort to diminish background reflection of light from the framed format 1, the framed portion has been blackened, as shown in, for example, FIG. 7A.

As shown in the FIG. 6A flow chart, in operation, after the fingerprint format is placed in the format holder and an identification card means is placed in a card reader, system command sequences are issued to the video scanner and the digitizer to commence and complete the scanning and digitizer functions.

Thus, the image of a fingerprint is video scanned to produce image data which is provided to a digitizer which converts the image data into digital image data which is stored in an addressable memory means (RAM) of the digitizer. To accomplish this, a sequence of commands are issued to the digitizer's "command port". This command sequence is specific to each end-user application. After these commands are issued, the digital fingerprint image and whitespace data generated by the scanning procedure and contained in memory in the digitizer, is ready for analysis.

Firmware Process Overview - The controlling firmware of the invention system has several components, each of which perform a specific task which, when combined, provide a series of processes that will take a fingerprint

sample and verify it against verification data to insure the authenticity of the provider of the sample. These processes include the following routines:

Comparison Data Retrieval Routine
Image Capture Routine
Image Sizing Routine
Algorithm Data Generation Routine
Verification Data Generation Routine
Data Confirmation Routine

Each of these routines are executed in sequence, and will be discussed in order. However, before the firmware verification process can commence, that set forth hereinabove must have been performed.

Comparison Data Retrieval Routine - This routine controls receipt of the Provider's verification data recorded on the identification card means, which is compared against data computed from the fingerprint sample to approve or fail the Provider's authenticity. The verification data could be encrypted and this will be discussed in a following disclosure section, along with an associated decryption function. The verification data (also termed "non-minutiae numerical identifier") recorded within the identification card means is read and stored in a 12 element array which is located in the processor of the invention system. This matrix has the same layout as the Generated Data Matrix which will be discussed subsequent to the following.

Image Frame Sizing Routine - This routine is generated subsequent to the Image Capture Routine which controls the operation of the video camera and the digitizer to capture the fingerprint image and whitespace data in memory. With reference to FIGS. 7A and 7B, this is accomplished as follows:

Note: "Whitespace" is defined as a greylevel equal to 13, 14, or 15.

a) Memory frame locations (128,Y), where $0 \leq Y \leq 255$ are inspected, when three consecutive rows of

whitespace are found, Y-TOP is defined as the current Y-value; and

b) Memory frame locations (128,Y), where 255 ≥ Y ≥ 0 are inspected, when three consecutive rows of whitespace are found, Y-BOTTOM is defined as the current Y-value.

c) With respect to FIGS. 8A and 8B, once Y-TOP and Y-BOTTOM values are established, the X-Axis Range of the fingerprint image data needs to be computed. This is accomplished by scanning (i.e., examining) each column (vertical line) to find three consecutive columns of whitespace. Once three columns are found, the next column containing a greylevel other than whitespace (i.e., black) is considered to be part of the Image.

Two X-Axis values, X-START and X-END, need to be set, to indicate the start and end memory data locations of the Image on the X-Axis, respectively. X-START is determined by scanning Frame Locations (X,Y), where 0 ≤ X ≤ 255 and Y-TOP ≤ Y ≤ Y-BOTTOM. This value indicates where the Image "starts" on the X-Axis. X-END is determined the same way, only reversing the X-Axis scan direction from 255 ≥ X ≥ 0, to determine where the Image "Ends" on the X-axis.

d) With respect to FIGS. 9A and 9B, now that the X-Axis range has been computed, the Y-Axis range of the FID needs to be computed. This is accomplished in a method similar to that used for the X-Axis Range.

Each row (horizontal line) is scanned, and, syncing on three consecutive whitespace rows, the next row that contains a greylevel other than whitespace is considered to be part of the image.

Two Y-Axis values, Y-START and Y-END, need to be set, to indicate the start and end memory data locations of the Image on the Y-Axis, respectively. Y-START is determined by scanning Frame Locations (X,Y), where X-START ≤ X ≤ X-END and Y-TOP ≤ Y ≤ Y-BOTTOM. Y-END is determined in similar fashion, only different being that the direction of scan along the Y-Axis is from Y-BOTTOM ≥ Y ≥ Y-TOP.

e) With respect to FIGS. 10A and 10B, all values generated must be validated to insure that an accurate image has been scanned and sized. If any of the following conditions fail, a "Poor Image Quality" error is generated, and the system recycles.

The conditions which will cause this error are:

i. Y-BOTTOM ≤ Y-TOP

ii. X-END ≤ X-START

iii. Y-END ≤ Y-START

If any of the above conditions are true, then the fingerprint sample provided to the Digitizer should be discarded and a new sample taken.

If none of the above error conditions exist, then the fingerprint sample is considered to have been accurately scanned and sized. The area within the memory frame where the fingerprint image data exists can be illustrated as shown in FIG. 10B.

Fingerprint Identity Window "Area of Analysis"

Prior to calling the mainline routine for the algorithm data generation routine (ADGR), locations must be set to describe the "window" within the fingerprint image data, stored in the memory frame, which is going to be analyzed. This "window" is a box, determined around an origin point defined as (XC,YC). XC and YC, or more appropriately called X-Center Line and Y-Center Line, are determined from values generated in the Image Sizing Routine, according to the following formulas:

$$XC = X\text{-}END - (X\text{-}END - X\text{-}START) / 3$$

$$YC = Y\text{-}END - (Y\text{-}END - Y\text{-}START) / 2$$

The difference between the two calculations is based upon the knowledge that the lower portion of a person's fingerprint (i.e., the portion containing the whirl) will be located closer to X-END than X-START. Thus, the XC value should start in the rightmost third of the print (hence, the division by 3) as that is where the whirl is likely to exist in the digitalized image. YC is simply

determined to be the standard Center Line between the two Y points on the frame's Y-Axis. Thus, assuming a print has been sized to exist from (50,50) to (200,150), (XC,YC) would be defined as (150,100).

Once (XC,YC) has been established, the "area of analysis" can easily be defined to the ADGR mainline routine. This area is defined depending on the specific needs of the end-user application, and is set by determining a "window-size".

The "window-size" is always an odd number. The "area of analysis" is then defined as XC ± DIFF and YC ± DIFF. DIFF is computed with the following formula:

$$DIFF = \frac{1}{2} (window\text{-}size - 1)$$

So, if the "window-size" is 73, the "area of analysis" would be appropriately defined as (XC ± 36, YC ± 36), or, in our example above, from (114,64) to (186,136).

Accordingly, the dimensional area of the fingerprint identity window is defined by predetermining a window-size for the fingerprint identity window and defining its dimensional area as from (XC - DIFF, YC - DIFF) to (XC + DIFF, YC + DIFF) where DIFF = ½ (window-size minus 1), wherein (XC - DIFF) = Xs, (YC - DIFF) = Ys, (XC + DIFF) = Xe, and (YC + DIFF) = Ye.

In addition to the X and Y Center Line values, there are four other variables which are used in Algorithm computations and these values are set forth hereinbelow and have been recited in connection with determining the dimensional area of the fingerprint identity window:

Description:	Symbol:	Value:
Window X-Axis Start	Xs	XC - DIFF
Window X-Axis End	Xe	XC + DIFF
Window Y-Axis Start	Ys	YC - DIFF
Window Y-Axis End	Ye	YC + DIFF

Once the proper values have been set, the "area of analysis" can be illustrated as shown in FIGS. 11A and 11B.

Algorithm Data Generation Routine - The Algorithm Data Generation Routine (ADGR) consists of a series of modules designed to generate 16 ridge-count values to be used in the computation of the Generated Data Matrix. The processing for each of these values will be discussed after the following presentation:

Algorithm Output Data

Key:
- S1 - Diagonal \ Absolute Count
- S2 - Diagonal / Absolute Count
- Yam - Y-Axis A-Range Maximum Absolute Count
- Ybm - Y-Axis B-Range Maximum Absolute Count
- Yaα - Y-Axis A-Range Average Count
- Yaß - Y-Axis A-Range Average Count
- Ybα - Y-Axis B-Range Average Count
- Ybß - Y-Axis B-Range Average Count
- Yc - Y-Axis Center Line Absolute Count
- Xam - X-Axis A-Range Maximum Absolute Count
- Xbm - X-Axis B-Range Maximum Absolute Count
- Xaα - X-Axis A-Range Average Count
- Xaß - X-Axis A-Range Average Count
- Xbα - x-Axis B-Range Average Count
- Xbß - X-Axis B-Range Average Count
- Xc - X-Axis Center Line Absolute Count

Algorithm Output Data:

01	02	03	04	05	06	07	08
S1	S2	Yam	Ybm	Yaα	Yaß	Ybα	Ybß
09	10	11	12	13	14	15	16
Yc	Xam	Xbm	Xaα	Xaß	Xbα	Xbß	Xc

Ridge counts are generated by examining the horizontal and vertical lines set forth hereinbelow, and counting the number of greylevel shifts from "white" (greylevels 13, 14, or 15) to "black" (greylevels 0 through 12).

The computation of the counts for the values of the Algorithm Output Data will now be described.

Value #1: S1 ; Diagonal \ Absolute Count (FIG. 12)

- -

This routine generates a count of ridges contained on the diagonal line drawn from point (Xs,Ys) to (Xe,Ye). Since the "window" is an absolute square, this relationship is a one-for-one increment along the X-Axis and Y-Axis, starting at Xs, and ending at Xe.

Value #2: S2 ; Diagonal / Absolute Count (FIG. 13)

- -

This routine generates a count of ridges contained on the diagonal line drawn from point (Xs,Ye) to (Xe,Ys). Since the "window" is an absolute square, this relationship is a one-for-one increment along the Y-Axis for each decrement along the X-Axis, starting at Xs, and ending at Xe.

Value #3: Yam ; Y-Axis A-Range Maximum Absolute Count (FIG. 14)

- -

This routine yields the highest number of ridges found on a horizontal line in the Y-Axis "A-Range". The Y-Axis "A-Range" is defined as: Ys ≤ horizontal line < YC.

In the example of FIG. 14, of the horizontal lines counted, the value of "Yam" would be set to "25", assuming that no other horizontal line contained a ridge count greater than 25. The "A-Range" is indicated with single-line borders.

Value #4: Ybm ; Y-Axis B-Range Maximum Absolute Count (FIG. 15)

- -

This routine yields the number of highest number of ridges found on a horizontal line in the Y-Axis "B-Range". The Y-Axis "B-Range" is defined as: YC < horizontal line ≤ Ye.

In the example of FIG. 15, of the horizontal lines counted, the value of "Ybm" would be set to "11", assuming that no other horizontal line contained a ridge

count greater than 11. The "B-Range" is indicated with single-line borders.

Values #5 & 6: Ya ; Y-Axis A-Range Average Count (FIG. 16)

- -

This routine yields the total number or ridges found on horizontal lines in the Y-Axis "A-Range". For computation purposes, this "overall total" is stored as two numbers, Yaα and Yaß. Yaα is the total number of 256 ridges in the "overall total" (i.e.: if Yaα is "2", then there are at least 512 ridges in the "overall total"). Yaß is the remaining number of ridges counted (i.e.: 6) which is always a number under 256. The Y-Axis "A-Range" is defined as: Ys ≤ horizontal line < YC.

In the example of FIG. 16, if the horizontal lines summed to 516, the value of "Yaα" would be set to "2", and the value of "Yaß" would be set to "4". The "A-Range" is indicated with single-line borders.

Values #7 & 8: Yb ; Y-Axis B-Range Average Count (FIG.17)

- -

This routine yields the total number of ridges found on horizontal lines in the Y-Axis "B-Range". For computation purposes, this "overall total" is stored as two numbers, Ybα and Ybß. Ybα is the total number of 256 ridges in the "overall total" (i.e.: if Ybα is "2", then there are at least 512 ridges in the "overall total"). Ybß is the remaining number of ridges counted (i.e.: 6) which is always a number under 256. The Y-Axis "B-Range" is defined as: YC < horizontal line ≤ Ye.

In the example of FIG. 17, if the horizontal lines summed to 300, the value of "Ybα" would be set to "1", and the value of "Ybß" would be set to "44". The "B-Range" is indicated with single-line borders.

Value #9: Yc ; Y-Axis Center Line Absolute Count (FIG. 18)

- -

This routine yields the number or ridges found on the horizontal line on the Y-Axis defined as YC, or Y-Center Line. This would be a whole number, such as 7, if 7 ridges were counted on the Y-Center Line.

Value #10: Xam ; X-Axis A-Range Maximum Absolute Count (FIG. 19)

- -

This routine yields the number of highest number of ridges found on a vertical line on the X-Axis "A-Range". The X-Axis "A-Range" is defined as: Xs ≤ vertical line < XC.

In the example of FIG. 19, of the vertical lines counted, the value of "Xam" would be set to "15", assuming that no other vertical line contained a ridge count greater than 15. The "A-Range" is indicated with single-line borders.

Value #11: Xbm ; X-Axis B-Range Maximum Absolute Count (FIG. 20)

- -

This routine yields the number of highest number of ridges found on a vertical line in the X-Axis "B-Range". The X-Axis "B-Range" is defined as: XC < vertical line ≤ Xe.

In the example of FIG. 20, of the horizontal lines counted, the value of "Xbm" would be set to "5", assuming that no other vertical line contained a ridge count greater than 5. The "B-Range" is indicated with single-line borders.

Values #12 & 13: Xa ; X-Axis A-Range Average Count (FIG. 21)

- -

This routine yields the total number or ridges found on the vertical lines in the X-Axis "A-Range". For computation purposes, this "overall total" is stored as two numbers, Xaα and Xaß. Xaα is the total number of 256 ridges in the "overall total" (i.e.: if Xaα is "2", then there are at least 512 ridges in the "overall total") Xaß is the remaining number of ridges counted (i.e.: 6) which is always a number under 256. The X-Axis "A-Range" is defined as: Xs ≤ vertical line < XC.

In the example of FIG. 21, if the vertical lines summed to 516, the value of "Xaα" would be set to "2", and the value of "Xaß" would be set to "4". The "A-Range" is indicated with single-line borders.

Values #14 & 15: Xb ; X-Axis B-Range Average Count (FIG. 22)

- -

This routine yields the total number of ridges found on vertical lines in the X-Axis "B-Range". For computation purposes, this "overall total" is stored as two numbers, Xbα and Xbß. Xbα is the total number of 256 ridges in the "overall total" (i.e.: if Xbα is "2", then there are at least 516 ridges in the "overall total"). Xbß is the remaining number or ridges counted (i.e.: 6) which is always a number under 256. The X-Axis "B-Range" is defined as: XC < vertical line ≤ Xe.

In the example of FIG. 22, if the vertical lines summed to 300, the value of "Xbα" would be set to "1", and the value of "Xbß" would be set to "44". The "B-Range" is indicated with single-line borders.

Value #16: Xc ; X-Axis Center Line Absolute Count (FIG. 23)

- -

This routine yields the number of ridges found on the vertical line on the X-Axis defined as XC, or X-Center

Line. This would be a whole number, such as 17, if 17 ridges were counted on the X-Center Line.

Generated Data Matrix

Key:		
	S1	- Diagonal \ Absolute Count
	S2	- Diagonal / Absolute Count
	Yma	- Y-Axis A-Range Maximum Absolute Count
	Ymb	- Y-Axis B-Range Maximum Absolute Count
	Ya	- Y-Axis A-Range Average Count
	Yb	- Y-Axis B-Range Average Count
	Yc	- Y-Axis Center Line Absolute Count
	Xma	- X-Axis A-Range Maximum Absolute Count
	Xmb	- X-Axis B-Range Maximum Absolute Count
	Xa	- X-Axis A-Range Average Count
	Xb	- X-Axis B-Range Average Count
	Xc	- X-Axis Center Line Absolute Count

Generated Data Matrix:

01	02	03	04	05	06	07	08	09	10	112
S1	S2	Yma	Ymb	Ya	Yb	Yc	Xma	Xmb	Xa	XbM

With reference to the Generated Data Matrix, the Verification Data Generation Routine will now be presented.

This routine takes the output of the Algorithm Data Generation Routine and creates the "Generated Data Matrix". For a full understanding of this process, refer to the two tables: "Algorithm Output Data" and "Generated Data Matrix", presented above.

The first element in the GDM (Generated Data Matrix) is equal to the value of the first number in the AOD (Algorithm Output Data). This element is known as "S1", or the "Diagonal \ Absolute Count".

The second element in the GDM is equal to the value of the second number in the AOD. This element is known as "S2", or the "Diagonal / Absolute Count".

The third element in the GDM is equal to the value of the third number in the AOD. This element is known as "Yam", or the "Y-Axis A-Range Maximum Absolute Count".

The fourth element in the GDM is equal to the value of the fourth number in the AOD. This element is known as "Ybm", or the "Y-Axis B-Range Maximum Absolute Count".

The fifth element in the GDM is a calculated value using the fifth and sixth numbers in the AOD. The calculated value can be indicated as follows:

value = (fifth * 256 + sixth) + (window-size ÷ 2)

In other words, the computation is equal to the fifth number in the AOD multiplied by 256, plus the sixth number in the AOD. The result is then divided by ½ the window size to give the calculated value. This element is known as "Ya", or the "Y-Axis A-Range Average Count".

The sixth element in the GDM is a calculated value using the seventh and eighth numbers in the AOD. The calculated value can be indicated as follows:

value = (seventh * 256 + eighth) ÷ (window-size + 2)

In other words, the computation is equal to the seventh number in the AOD multiplied by 256, plus the eighth number in the AOD. The result is then divided by ½ the window size to give the calculated value. This element is known as "Yb", or the "Y-Axis B-Range Average Count".

The seventh element in the GDM is equal to the value of the ninth number in the AOD. This element is known as "Yc", or the "Y-Axis Center Line Absolute Count".

The eighth element in the GDM is equal to the value of the tenth number in the AOD. This element is known as "Xam", or the "X-Axis A-Range Maximum Absolute Count".

The ninth element in the GDM is equal to the value of the eleventh number in the AOD. This element is known as "Xbm", or the "X-Axis B-Range Maximum Absolute Count".

The tenth element in the GDM is a calculated value using the twelfth and thirteenth numbers in the AOD. The calculated value can be indicated as follows:

value = (twelfth * 256 + thirteenth) + (window-size + 2)

In other words, the computation is equal to the twelfth number in the AOD multiplied by 256, plus the thirteenth number in the AOD. The result is then divided by ½ the window size to give the calculated value. This element is known as "Xa", or the "X-Axis A-Range Average Count".

The eleventh element in the GDM is a calculated value using the fourteenth and fifteenth numbers in the AOD. The calculated value can be indicated as follows:

value = (fourteenth * 256 + fifteenth) + (window-size + 2)

In other words, the computation is equal to the fourteenth number in the AOD multiplied by 256, plus the fifteenth number in the AOD. The result is then divided by ½ the window size to give the calculated value. This element is known as "Xb", or the "X-Axis B-Range Average Count".

The twelfth element in the GDM is equal to the value of the sixteenth number in the AOD. This element is known as "Xc", or the "X-Axis Center Line Absolute Count".

Fingerprint Identification System Data Confirmation Routine

This routine is responsible for comparing the Comparison Data Matrix (CDM) against the Generated Data Matrix (GDM,) and determining if the fingerprint sample given by the Provider mathematically matches the verification data on the Provider's portable personnel identification means.

Each element of the CDM is compared against its counterpart in the GDM. That is, the first element of the CDM is compared against the first element of the GDM, the

second element of the CDM is compared against the second element in the GDM, and so on.

The absolute difference between elements is limited to specific pre-defined "tolerances". These tolerances will vary from application to application, depending on the needs of the end-user. An end-user who wants very strict regulation would have lower tolerances than an end-user who wants average regulation. In other words, one end-user may want ±3 tolerance whereas another might want ±1 tolerance.

As an example, the first through seventh elements will always have one level of tolerance higher than the eighth through twelfth elements. In other words, if the eighth through twelfth elements are measured with a ±2 tolerance, then the first through seventh elements will have a tolerance of ±3.

To determine whether or not a fingerprint sample is approved, a "confidence level" has to be achieved. This confidence level starts at zero. When each CDM/GDM element is compared, and the difference falls within the acceptable tolerance, then the confidence level is increased by 8.33%.

The actual confidence level that must be achieved in order for a fingerprint to be "approved" is again determined by the specific application. One end-user might want a higher confidence level than another end-user.

After all elements have been compared, and the confidence level is determined, a flag is set to indicate whether or not the sample has "passed" the confirmation process.

The entire process (2 - Image Capture through 6 - Data Confirmation) is repeated up to 10 times.

If a sample is confirmed two consecutive times, then the fingerprint sample is "approved", an appropriate confirmation message is generated for the Obtainer to view, and the device recycles.

If a sample is rejected two consecutive times, then the fingerprint sample is "failed", an appropriate

rejection message is generated for the Obtainer to view, and the device recycles.

If in the ten process cycles the firmware cannot obtain two consecutive "passes" or "failures", then the fingerprint sample is "unable to verify", an appropriate message is generated for the Obtainer to view, and the device recycles.

It should be apparent to any person skilled in the art to which this invention pertains that the disclosure set forth hereinabove with respect to the calculation of the plurality of counts, with reference to either a diagonal line or a horizontal line or a vertical line, pertains to a line of memory data contained within the fingerprint identity window area being analyzed.

The foregoing has been disclosed with respect to a preferred method and system wherein the Generated Data Matrix provides 24 bytes of fingerprint identification data, each element of the GDM containing 2 bytes of verification data. The 24 byte non-minutiae digitized numerical identifier is recordable within the confines of a portable personnel identification means and in particular, the magnetic stripe of a credit card to allow the credit card to be used as an identification card for entitling the user to certain services, as for example, charged purchases and check cashing. This digitized numerical identifier can also be stored in a memory means included in a smart card.

As to the particular application of the invention system and methods for providing a 24 byte non-minutiae digitized numerical identifier which is recordable within the magnetic stripe of a credit card to allow the credit card to be used as a portable personnel identification card, regulations of the American National Standards for financial services, financial transaction cards magnetic stripe encoding, limit the magnetic stripe and coding as follows:

TRACK 1 maximum of 79 alphanumeric characters

TRACK 2 maximum of 40 characters, numeric only
TRACK 3 maximum of 107 alphanumeric characters

Various other market applications of the present invention system and methods are as follows:

Retail Credit Card

Government-federal/State/Local
Used to identify the voter; controlling multiple voting Drivers License; control verification of individual for legal drinking age.
System could be used in control of aliens on green cards and work visa's
Social Security cards..verification of holder for check cashing requirements.
Military ID cards for all branches.
Control of welfare recipients and check cashing.

Security Market
Banking industry..Automatic Tellers (ATM's), safety deposit boxes.

Professional Market
Medical...ID cards.

Education Market
College entrance exams.
Legal Bar Exams.

Other Markets
Passports.
Prisons.
Security..Computer access as well as commercial use.

VARIABLE RESOLUTION

The foregoing presentation of the invention methods for image sizing, image framing, and that set forth with respect to defining a fingerprint identity window, bear reference to a resolution area base 256. It should be apparent that the present invention is not limited to this exemplary resolution area since it is well within the teachings and scope of the present invention to employ a resolution area base 512. Accordingly, it will be apparent to those skilled in the art in light of the foregoing disclosure that the invention should not be limited to a resolution area base 256.

ENCRYPTION/DECRYPTION

Verification String encryption routines can take a myriad of forms. Each scheme is application dependent, meaning that a scheme used for one application will not be used in a similar application - thus reducing the possibility of fraud. Since the scheme for each application is different, and bound in the verification firmware EPROMS, the possibility of unauthorized card duplication is reduced, as duplicated cards for one application would not yield valid verification data in another application. Two exemplary encryption schemes are as follows:

Scheme 1: Digit Reversal Scheme

This "encryption scheme" takes each of the twelve numbers in the Verification String and reverses the digits. In other words, if the Verification String contains the following numbers:

01 40 36 24 22 05 10 18 14 21 040

then the "encrypted" data would appear as follows:

10 04 63 42 22 50 01 81 41 12 400

To "decrypt" the data in an application program, the programmer need only reverse the digits back to obtain the original numbers.

Scheme 2: Digit Complement Scheme

This "encryption scheme" operates on all 24 digits of the Verification String as a whole, treating each digit as a separate entity. Each digit is subtracted from nine (9) to achieve a "complement" value. For instance:

01 40 36 24 22 05 10 18 14 21 040

would appear as follows once encrypted:

98 59 63 75 77 94 89 81 85 78 959

This complement scheme has the same affect as taking each of the twelve numbers and subtracting each number from ninety-nine (99) to achieve the "encrypted" value.

To reverse the process, the user only need to subtract 9 from each of the 24 encrypted digits to achieve the original number (ignoring the negative sign).

As stated above, data encryption will vary from application to application, to avoid multiple applications from having similar verification data, and thus introducing potential misuse of the encrypted verification data. The encryption method is decided in advance, and appropriate decryption logic is programmed into the Comparison Data Retrieval Routine, such that the decrypter logic and means of implementation are contained in the BCC52 processor of the system invention.

As to the implementation of the encryption scheme aspect of the present invention, in addition to providing a fingerprint sample, the Provider also presents identification card means (i.e., identification card with a magnetic stripe) which contains his or her encrypted verification data (i.e., encrypted digitized numerical identifier), the identification card is then placed in the card reader for retrieval and decryption of the "comparison data".

Upon decryption, the "comparison data" is stored in a 12 element array, known as the "Comparison Data Matrix", which has the same layout as the "Generated Data Matrix" presented hereinbefore.

If any errors are encountered during this retrieval process, then an appropriate error message is generated and the system recycles. Such error messages are specific to the individual application (i.e., a system with a magnetic stripe card reader would have a "Card Reader Error" or a "Channel Read Error" error message). Furthermore, the encrypted identifier could also be included on a check payable within a check cashing identity verification application of the present invention.

As set forth in the appended claims, the present invention is applicable to: recording an encrypted or non-encrypted non-minutiae digitized numerical identifier

within the confines of a portable personnel identification means, personal to a person, such as a credit card or a smart card, identity verification of a person to be identified with or without an encryption scheme, and payable check verification of identity of payee, with or without encryption.

As to the recording application, two services could be performed: (1) direct or indirect personal contact with the persons to be identified, deriving non-minutiae digitized numerical identifiers indicative of the fingerprints of such persons, and recording the non-minutiae digitized numerical identifiers within identification means, personal to such persons; or (2) performing such a service but providing the derived non-minutiae digitized numerical identifiers to another party for the performance of the recording procedure.

As to the Identity Verification Application of the present invention, this could be accomplished with direct or indirect personal contact with persons to be identified.

With regard to the payable check verification of identity of a check payee, the check payable could include a numerical identifier to be verified with a digitized numerical identifier indicative of a fingerprint of a check payee named on the check payable, or preferably no numeric identifier would be included on the check payable and verification of the identity of the person submitting the check payable in a check cashing application would be accomplished by verification of comparison of a non-minutiae digitized numerical identifier indicative of a fingerprint of a person submitting the check for cashing, with the numerical identifier contained within a portable personnel identification means submitted by such person for identification as the check payee of the check payable.

With reference back to the identification verification application of the present invention, where verification of identity is accomplished by comparing the

numerical identifier of identification means with the non-minutiae digitized numerical identifier derived from a fingerprint of such person to be identified, upon finding non-verification, the portable personnel identification means would be withheld by the invention system, or in the case where a smart card is presented as the identification means, the functional integrity of such smart card could be destroyed by known techniques and devices incorporated into the system invention.

Thus, it is apparent that there has been provided, in accordance with the invention, an identification system that fully satisfies the objectives, aims and advantages set forth above. While the invention methods have been described in conjunction with specific applications thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended to embrace all such alternatives, modifications and variations which fall within the spirit and scope of the appended method claims.

The terms and expressions which have been employed in the foregoing specification are used therein as terms of description and not solely of limitation, and there is no intention, in the use of such terms and expressions, of excluding equivalents of the features shown and described or portions thereof, it being recognized that the scope of the invention is defined and limited only by the appended method claims.

FINGERPRINT IDENTIFICATION SYSTEM INVENTION

A description of the system invention will now be presented with reference to FIGS. 24 - 32 which are illustrative of the system invention, and FIGS. 4 - 6B and FIGS. 33 and 34 which provide flow charts which are descriptive of the operation control of the system invention.

FIG. 24 is a block diagram of the invention system which shows the basic interconnection of the system components including the video camera 4, and the accessories LCD display 40, printer means 50, and PPI/MS Reader 60. An illustrative power supply means PS for providing appropriate voltage supply to the system components is also shown.

The system invention can be embodied in three specific configurations which differ from each other as to the application of the system invention and the components utilized for a respective application. Each of the three embodiments incorporate the following: an inkless framed format holder means 3, video scanning means 4, lens 5, digitizer 10, processor 20, LCD driver means 30, a four-slot motherboard bus connector Z8, and a portable personnel identification card reader means 60.

Prior to presenting a description for each embodiment of the system invention, the basic system as depicted in FIG. 24 will now be described.

Video scanner 4 scans an inkless format means providing an image of a fingerprint of a person to be identified, after this fingerprint image format 1 is placed within the inkless format holder means 3 which automatically positions the format 1 in relation to the video scanner 4 in such a way that the position is predetermined and will be reestablished each time that a print format means is placed before the video scanner, thus insuring that a subsequent scanning operation will always produce consistent and reliable field of scan results.

As shown in FIG. 24, the video output of scanner 4 is connected to digitizer 10 via a shielded coaxial cable 9. The video scanner 4 receives power from the 120 volts AC supply, and a ground is provided via line 7 from pin 2 of Z8. In operation, the video scanner scans the image of a fingerprint provided on an inkless means 2 to produce fingerprint image data and whitespace data which is outputed to the video digitizer board 10.

The primary function of the video digitizer board 10 is to convert the fingerprint image and whitespace data signals from the video scanner into digital image data i.e., numerical data, which digital image data is stored in an addressable memory means, RAM, included in the digitizer 10. Thus, the stored digital image data is then available to the system program-controlled processor 20 for evaluation of the scanned image data information.

The scanned image data information contained in the video camera output signal is made up of discrete points of picture elements, commonly called pixels. Each pixel varies in brightness, depending on the image scanned, through a range of "grey levels" from black to white. In digitizer 10, these grey levels are separated into 16 numerical values from 0 (black) to 15 (white). Each horizontal line of the image data being viewed contains 256 pixels and the circuitry of the digitizer samples 256 lines. This results in 65,536 pixels or discrete numerical values that the digitizer must store in its random access memory means. Since the pixels are supplied in a scanning sequence (from left to right in the viewed image) it is necessary that the sampling in some subsequent storage of the pixel values be synchronized with camera scanning sequence. Signals are provided, along with the fingerprint image and whitespace data outputed from the camera. These combined signals, image and sync, are commonly referred to as "composite video".

Circuit means of the digitizer functions to extract both horizontal (line) and vertical (frame) synchronization signals. Other circuitry of the digitizer 10 allows the system microprocessor 20 to control a variety of functions under software control. The primary function of the digitizer 10, as referred to earlier, is to convert the scanned image data into numerical values for later evaluation by the software controlled processor. The operation of the digitizer 10 of the invention is well known to those skilled in the art and a specific

designation of a digitizer utilized in the system invention is presented hereinafter along with designations for the other components incorporated into the present system.

The program-controlled processor means 20 selectively analyzes a plurality of different fingerprint pattern parts of the digital image data contained in the digitizer, and the processor includes means for accomplishing the inventive methods set forth in the foregoing, such as means for computing a ridge count for each of the plurality of selectively analyzed different fingerprint pattern parts, means for compiling a data matrix comprised of ridge counts computed for these different fingerprint pattern parts, means to provide a non-minutiae digitized numerical identifier indicative of the image of the fingerprint of a person to be identified, and means for comparing the numerical identifier provided by the card reader 60 with the non-minutiae digitized numerical identifier, to verify the identity of a person to be identified. Reference to the foregoing description will also provide information as to the other inventive methods of the invention such as that set forth for Image Capture, Image Sizing and the defining of a fingerprint identity window.

The flow charts illustrated in FIGS. 4 - 6B, 33 and 34 provide the system operations performed by the processor means 20 under software control.

The LCD Driver means 30 communicates with the processor 20 via J4 and Z8, and its output is connected to LCD display means 40 via connector J6.

Printer 50 is connected to processor 20 via connector J5.

A portable personnel identification means magnetic-stripe reader 60 is connected to processor 20 via RS-232-C, 25 pin serial connector 8 and connector J1. This reader is provided with a simple reset circuit (not shown) to initialize the control microprocessor when power is first supplied to the system.

Appendix A attached hereto describes the software utilized in the system of the invention.

The disclosure set forth hereinabove and attached hereto, with reference to the drawings, will enable any person skilled in the art to which this invention pertains, to assemble and operate the system invention in accordance with the inventive methods provided herein.

The specific circuitry incorporated in the particular embodiment of an automatic fingerprint identification system constructed in accordance with the present invention and described with reference to the respective drawings, can be constructed from discrete elements more advantageously as from integrated circuits. The following Table lists examples of such components.

TABLE A

Component	Description
Inkless material	Identicator Corporation
Video camera	Associated Systems Model # TC1886,
Camera lens	16 mm, F/1.6 (no iris)
PPI/MS card reader	American Magnetics Corporation-Model 101
Smart card reader	Microcard Technologies
Video digitizer	VIP Ltd - Model #D10010
Processor	Micromint, Inc. - Model # BCC52C
LCD Driver	Micromint, Inc. - BCC25, BCC52C ROM A&B, MB04 Passive Backplane
Printer	Printer Products - Dot Matrix Printer-40 columns

The MBO 4-slot motherboard Z8 is an 8 BUS configuration. The processor BCC52C contains RAM/EPROM, an EPROM programmer, 3 parallel ports, and 2 serial ports.

SYSTEM EMBODIMENTS

FIG. 29 illustrates a first embodiment of the system invention which incorporates a PPI/MS Reader 60, card entry means 70 and an LCD display window 80 to display

messages from LCD assembly 40, this embodiment being devoid of a printer. The fingerprint format holder means 3 for positioning a fingerprint format in a predetermined scanned position is shown. This holder means 3 is fixedly attached to the faceplate FP of the housing. The faceplate FP includes an appropriately positioned, square-hole, around which the format holder means is attached in a predetermined position. This allows the video camera 4 to have viewing access to the fingerprint image contained within a fingerprint format means 1 after it is placed within the fingerprint format holder 3.

The faceplate has mounted on its inner side electroeluminance lamps which illuminate the field of view of the video camera. One of the lamps is mounted in a predetermined position, angled downwardly from the top of the hole, and the other lamp is appropriately mounted and angled from the bottom of the hole.

FIG. 30 illustrates a second embodiment of the system invention in the application wherein a smart card is provided as the portable personnel identification card means. A smart card reader means (not shown) replaces the PPI/MS reader 60 in the basic system circuitry, and a smart card access slot means 90 is provided to allow entry of the smart card into the smart card reader. This embodiment incorporates the same LCD components, and is devoid of a printer.

FIG. 31 illustrates a third embodiment of the system invention application to payable check verification of identity of a check payee, as set forth hereinbefore. This embodiment employs an identification card reader means 60 and associated means 70, or can employ an appropriate smart card reader means when a smart card is used as the personnel identification card means. Printer means 50 is incorporated in this embodiment to print on a check payable an identification verification message, or any other message provided by this system invention. Slots 92 and 94 are provided to allow access to and from the printer which

is accomplished by inserting a check payable into slot 94, and after the system operation is completed, the check will be returned via slot 92.

The specific operations of each of the three embodiments described above is set forth in the foregoing description and in the appended claims.

Thus, it is apparent that there has been provided, in accordance with the system invention, a non-minutiae automatic fingerprint identification system that fully satisfies the objectives, aims and advantages set forth above. While the invention system has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications and variations will be apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended to embrace all such alternatives, modifications and variations which fall within the spirit and scope of the appended system claims.

1. A method for providing identification of a person comprising the steps of:

a) obtaining an image of a fingerprint of said person, said image being provided on an inkless means which when touched by a finger of the said person causes immediate development of an image of the fingerprint of said finger in a black and white appearance,

b) video scanning said image of a fingerprint provided on said inkless means to produce image data and digitizing said image data to produce a non-minutiae digitized numerical identifier indicative of said fingerprint, and

c) recording said non-minutiae digitized numerical identifier within the confines of a portable personnel identification means, personal to said person.

2. A method as defined in Claim 1 further comprising: recording said non-minutiae digitized numerical identifier within the magnetic stripe of a credit card personal to said person.

3. A method as defined in Claim 1 further comprising: recording said non-minutiae digitized numerical identifier within a smart card, personal to said person, by storing the said non-minutiae digitized numerical identifier in a memory means included in said smart card.

4. A method as defined in Claim 1 further comprising: digitizing the said image data to produce a non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data.

5. A method as defined in Claim 1 further comprising: digitizing the said image data to produce a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data.

6. A method as defined in Claim 2 further comprising: recording within said magnetic stripe of a credit card personal to said person a non-minutiae digitized numerical identifier having less than 100 bytes of fingerprint identification data.

7. A method as defined in Claim 2 further comprising: recording within said magnetic stripe of a credit card, personal to said person, a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data.

8. A method as defined in Claim 3 further comprising: recording within said smart card, personal to said person, a non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data, by storing said data in a memory means included in the said smart card.

9. A method as defined in Claim 3 further comprising: recording within said smart card, personal to said person, a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data, by storing said data in a memory means included in the said smart card.

10. A method for providing identification of a person comprising the steps of:

a) requesting and receiving from a person to be identified a fingerprint, said fingerprint being provided via the use of an inkless means which when touched by a finger of said person causes immediate development of an image of the fingerprint of said finger in a black and white appearance,

b) video scanning said image of a fingerprint provided on said inkless means to produce image data and digitizing said image data to produce a non-minutiae digitized numerical identifier indicative of said fingerprint, and

c) recording said non-minutiae digitized numerical identifier within the confines of a portable personnel identification means, personal to said person.

11. A method as defined in Claim 10 further comprising: recording said non-minutiae digitized numerical identifier within the magnetic stripe of a credit card personal to said person.

12. A method as defined in Claim 10 further comprising: recording said non-minutiae digitized numerical identifier within a smart card, personal to said person, by storing the said non-minutiae digitized numerical identifier in a memory means included in said smart card.

13. A method as defined in Claim 10 further comprising: digitizing the said image data to produce a non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data.

14. A method as defined in Claim 10 further comprising: digitizing the said image data to produce a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data.

15. A method as defined in Claim 11 further comprising: recording within said magnetic stripe of a credit card personal to said person a non-minutiae digitized numerical identifier having less than 100 bytes of fingerprint identification data.

16. A method as defined in Claim 11 further comprising: recording within said magnetic stripe of a credit card, personal to said person, a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data.

17. A method as defined in Claim 12 further comprising: recording within said smart card, personal to said person, a non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data, by

storing said data in a memory means included in the said smart card.

18. A method as defined in Claim 12 further comprising: recording within said smart card, personal to said person, a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data, by storing said data in a memory means included in the said smart card.

19. A method as defined in Claim 10, further comprising: prior to step c), encrypting said non-minutiae digitized numerical identifier and recording the encrypted digitized numerical identifier within the confines of said portable personnel identification means.

20. A method as defined in Claim 11, further comprising: prior to step c), encrypting said non-minutiae digitized numerical identifier and recording the encrypted digitized numerical identifier within said magnetic stripe of said credit card.

21. A method as defined in Claim 12, further comprising: prior to step c), encrypting said non-minutiae digitized numerical identifier and recording the encrypted digitized numerical identifier in said memory means of said smart card.

22. A method as defined in Claim 13, further comprising: encrypting said non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier within the confines of said portable personnel identification means.

23. A method as defined in Claim 14, further comprising: encrypting said non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier within the confines of said portable personnel identification means.

24. A method as defined in Claim 15, further comprising: encrypting said non-minutiae digitized numerical identifier having less than 100 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier within said magnetic stripe of said credit card.

25. A method as defined in Claim 16, further comprising: encrypting said non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier within said magnetic stripe of said credit card.

26. A method as defined in Claim 17, further comprising: encrypting said non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier in said memory means of said smart card.

27. A method as defined in Claim 18, further comprising: encrypting said non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier in said memory means of said smart card.

28. A method of verifying the identity of a person comprising the steps of:

a) obtaining a fingerprint of a person to be identified provided via the use of an inkless means which when touched by a finger of said person causes immediate development of an image

of the fingerprint of said finger in a black and white appearance,

b) providing a portable personnel identification means, personal to said person, having recorded therewith a non-minutiae numerical identifier which identifies the fingerprint of the said finger of said person,

c) reading said numerical identifier recorded on said portable personnel identification means, and storing in memory the said numerical identifier,

d) video scanning said image of said fingerprint provided by said inkless means to produce image data and digitizing said image data to produce a non-minutiae digitized numerical identifier indicative of said fingerprint,

e) comparing the numerical identifier of said identification means stored in memory with said non-minutiae digitized numerical identifier, to verify the identity of said person.

29. A method as defined in Claim 28, further comprising as to step a) above: using the index finger of said person to be identified to provide said fingerprint.

30. A method as defined in Claim 28, further comprising as to step a) above: using the thumb of said person to be identified to provide said fingerprint.

31. A method as defined in Claim 28, further comprising as to step b) above: providing a credit card as said portable personnel identification means, personal to said person.

32. A method as defined in Claim 28, further comprising as to step b) above: providing a smart card as said portable personnel identification means, personal to said person.

33. A method as defined in Claim 28, further comprising as to step d) above: using a video camera to video scan the said image of the said fingerprint provided on the said inkless means.

34. A method as defined in Claim 28, further comprising the step of: prior to digitizing the said image data, storing in a random-access memory means the scanned image of the said fingerprint provided on the said inkless means.

35. A method as defined in Claim 28, further comprising: displaying verification of the identity of said person.

36. A method as defined in Claim 35, further comprising: displaying non-verification of the identity of the said person.

37. A method as defined in Claim 36, further comprising: withholding said portable personnel identification means upon occurrence of non-verification of the identity of said person.

38. A method as defined in Claim 37, further comprising: withholding a credit card provided as said personal personnel identification means upon occurrence of non-verification of the identity of said person.

39. A method as defined in Claim 37, further comprising: withholding a smart card provided as said personal personnel identification means upon occurrence of non-verification of the identity of said person.

40. A method as defined in Claim 36, further comprising: destroying the functional integrity of a smart card provided as said personal personnel identification means upon occurrence of non-verification of the identity of said person.

41. A method as defined in Claim 1, further comprising: prior to step c), encrypting said non-minutiae digitized numerical identifier and recording the encrypted digitized numerical identifier within the confines of said portable personnel identification means.

42. A method as defined in Claim 2, further comprising: prior to step c), encrypting said non-minutiae digitized numerical identifier and recording the encrypted digitized numerical identifier within said magnetic stripe of said credit card.

43. A method as defined in Claim 3, further comprising: prior to step c), encrypting said non-minutiae digitized numerical identifier and recording the encrypted digitized numerical identifier in said memory means of said smart card.

44. A method as defined in Claim 4, further comprising: encrypting said non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier within the confines of said portable personnel identification means.

45. A method as defined in Claim 5, further comprising: encrypting said non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier within the confines of said portable personnel identification means.

46. A method as defined in Claim 6, further comprising: encrypting said non-minutiae digitized numerical identifier having less than 100 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier within said magnetic stripe of said credit card.

47. A method as defined in Claim 7, further comprising: encrypting said non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier within said magnetic stripe of said credit card.

48. A method as defined in Claim 8, further comprising: encrypting said non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier in said memory means of said smart card.

49. A method as defined in Claim 9, further comprising: encrypting said non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data and recording the encrypted digitized numerical identifier in said memory means of said smart card.

50. A method for verifying the identity of a person comprising the steps of:

a) providing a fingerprint of a person to be identified,

b) providing a portable personnel identification means, personal to said person, having an encrypted numerical identifier which identifies said fingerprint of the said person,

c) decrypting said encrypted numerical identifier of said portable personnel identification means to provide a decrypted numerical identifier,

d) video scanning the said fingerprint and digitizing the image data of the scanned fingerprint to produce a non-minutiae digitized numerical identifier indicative of said fingerprint, and

e) comparing said non-minutiae digitized numerical identifier with said decrypted numerical identifier to verify the identity of said person.

51. A method as defined in Claim 50 further comprising: providing said fingerprint of a person to be identified via the use of an inkless means which when touched by a finger of said person causes immediate development of an image of the said fingerprint in a black and white appearance.

52. A method as defined in Claim 50, further comprising as to step a) above: using the index finger of said person to be identified to provide said fingerprint.

53. A method as defined in claim 50, further comprising as to step a) above: using the thumb of said person to be identified to provide said fingerprint.

54. A method as defined in Claim 50, further comprising as to step b) above: providing a credit card as said portable personnel identification means, personal to said person.

55. A method as defined in Claim 50, further comprising as to step b) above: providing a smart card as said portable personnel identification means, personal to said person.

56. A method as defined in Claim 50, further comprising as to step d) above: using a video camera to video scan the said fingerprint.

57. A method as defined in Claim 50, further comprising the step of: prior to digitizing said image data, storing in a random-access memory means the said image data of the scanned fingerprint.

58. A method as defined in Claim 50, further comprising: displaying verification of the identity of said person.

59. A method as defined in Claim 58, further comprising: displaying non-verification of the identity of the said person.

60. A method as defined in Claim 59, further comprising: withholding said portable personnel identification means upon occurrence of non-verification of the identity of said person.

61. A method as defined in Claim 60, further comprising: withholding a credit card provided as said personal personnel identification means upon occurrence of non-verification of the identity of said person.

62. A method as defined in Claim 60, further comprising: withholding a smart card provided as said personal personnel identification means upon occurrence of non-verification of the identity of said person.

63. A method as defined in Claim 59, further comprising: destroying the functional integrity of a smart card provided as said personal personnel identification means upon occurrence of non-verification of the identity of said person.

64. A method as defined in Claim 1, further comprising as to step a) above: using the index finger of said person to be identified to provide said fingerprint.

65. A method as defined in claim 1, further comprising as to step a) above: using the thumb of said person to be identified to provide said fingerprint.

66. A method as defined in Claim 1 further comprising as to step a) above: using a toe of a person to be identified to provide an identification print.

67. A method as defined in Claim 10, further comprising as to step a) above: using the index finger of said person to be identified to provide said fingerprint.

68. A method as defined in claim 10, further comprising as to step a) above: using the thumb of said person to be identified to provide said fingerprint.

69. A method as defined in Claim 10 further comprising as to step a) above: using a toe of a person to be identified to provide an identification print.

70. A method as defined in Claim 28, further comprising as to step a) above: using a toe of a person to be identified to provide an identification print.

71. A method as defined in Claim 50, further comprising as to step a) above: using a toe of a person to be identified to provide an identification print.

72. A method for the automatic non-minutiae identification of a fingerprint image comprising in combination:

a) scanning an image of a fingerprint of a person to be identified;

b) storing in an addressable memory means image data produced from scanning said image;

c) selectively analyzing a plurality of different fingerprint pattern parts of the stored image data and computing a ridge count for each of said plurality of fingerprint pattern parts; and

d) compiling a data matrix comprised of a plurality of ridge counts computed for the said plurality of fingerprint pattern parts to provide a non-minutiae digitized numerical identifier indicative of said image of a fingerprint of a person to be identified.

73. A method as defined in Claim 72 further comprising: providing said fingerprint image via the use of an inkless means which when touched by a finger of said person causes immediate development of said image of a fingerprint of the said person.

74. A method as defined in Claim 73 further comprising: providing a non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data.

75. A method as defined in Claim 73 further comprising: providing a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data.

76. A method as defined in Claim 74 further comprising: encrypting said non-minutiae digitized numerical identifier and recording the encrypted digitized numerical identifier within the confines of a portable personnel identification means personal to said person to be identified.

77. A method as defined in Claim 75 further comprising: encrypting said non-minutiae digitized numerical identifier and recording the encrypted digitized numerical identifier within the confines of a portable personnel identification means personal to said person to be identified.

78. A method as defined in Claim 73 further comprising: providing said fingerprint image by using the index finger of said person.

79. A method as defined in Claim 73 further comprising: providing said fingerprint image by using the thumb of said person.

80. A method as defined in Claim 73 further comprising: providing said image by using a toe of said person.

81. A method for the automatic non-minutiae identification of a fingerprint of a person to be identified, comprising the steps of:

a) scanning an image of a fingerprint and producing fingerprint image data and whitespace data;

b) storing in an addressable memory means said fingerprint image and whitespace data; and

c) determining the location of the said fingerprint image data stored in said memory means with the said whitespace data.

82. A method as defined in Claim 81, further comprising: defining a fingerprint identity window within said fingerprint image data.

83. A method as defined in Claim 82, further comprising: defining said fingerprint identity window by determining the dimensions of said window around an origin point defined as (XC, YC), wherein XC = X-END minus (X-END minus X-START) divided by 3, and YC = Y-END minus (Y-END minus Y-START) divided by 2.

84. A method as defined in Claim 81, further comprising as to step c):

image framing the said fingerprint image and whitespace data to a predetermined dimension, and establishing Y-TOP and Y-BOTTOM values along the Y-axis of said predetermined dimension;

computing the X-Axis Range of the fingerprint image data contained in the framed image data by determining two X-axis values, said X-axis values being X-START and X-END, wherein X-START indicates the memory data location where the fingerprint image data starts on the X-axis, and X-END indicates the memory data location where the fingerprint image data ends on the X-axis;

computing the Y-Axis Range of the fingerprint image data contained in the framed image data by

determining two Y-axis values, said Y-axis values being Y-START and Y-END, wherein Y-START indicates the memory data location where the fingerprint image data starts on the Y-axis, and Y-END indicates the memory data location where the fingerprint image data ends on the Y-axis; and

determining the dimensional area of said fingerprint image data by utilizing said X-START, X-END, Y-START and Y-END values.

85. A method as defined in Claim 84, further comprising: defining a fingerprint identity window within said fingerprint image data.

86. A method as defined in Claim 85, further comprising: defining said fingerprint identity window by determining the dimensions of said window around an origin point defined as (XC, YC), wherein XC = X-END minus (X-END minus X-START) ÷ 3, and YC = Y-END minus (Y-END minus Y-START) ÷ 2.

87. A method as defined in Claim 86, further comprising:

defining said whitespace data as having a predetermined greylevel value;

defining said fingerprint image data as having a second predetermined greylevel value distinct from that defined for the said whitespace data;

as to said image framing, examining memory data locations (128,Y) where $0 \leq Y \leq 255$, and upon finding three consecutive rows of whitespace data, defining Y-TOP as the latter examined data row Y-axis value, and examining memory data locations (128,Y) where $255 \geq Y \geq 0$ and upon finding three consecutive rows of whitespace data, defining Y-BOTTOM as the last examined data row Y-axis value;

computing the X-Axis Range of the framed image data to indicate the start and end memory locations of the fingerprint image data on the X-axis by determining X-START and X-END X-axis values, wherein X-START is determined by

examining memory data locations (X,Y) where $0 \leq X \leq 255$ and Y-TOP $\leq$ Y $\leq$ Y-BOTTOM, by detecting three consecutive columns of whitespace data and a next column having a greylevel value equal to said second predetermined value and considering the memory data location of said next column to be a first part of said fingerprint image data along the X-axis, and wherein X-END is determined in similar manner as for said X-START value but in an opposite direction from $255 \geq X \geq 0$ along the X-axis so that said X-END value indicates the memory data location along the X-axis where the fingerprint image data ends;

computing the Y-Axis Range of the framed image data to indicate the start and end memory locations of the fingerprint image data on the Y-axis by determining Y-START and Y-END Y-axis values, wherein Y-START is determined by memory data locations (X,Y) where X-START $\leq$ X $\leq$ X-END and Y-TOP $\leq$ Y $\leq$ Y-BOTTOM, by detecting three consecutive rows of whitespace data and a next row having a greylevel value equal to said second predetermined value and considering the memory data location of said next row to be a first part of said fingerprint image along the Y-axis, and wherein Y-END is determined in similar manner as for said Y-START value but in an opposite direction from Y-BOTTOM $\geq$ Y $\geq$ Y-TOP along the Y-axis so that said Y-END value indicates the memory data location along the Y-axis where the fingerprint image data ends;

defining said fingerprint identity window by determining the dimension of said window around an origin point defined as (XC,YC) wherein:

XC = X-END minus (X-END minus X-START) + 3 and

YC = Y-END minus (Y-END minus Y-START) + 2; and

further defining the dimensional area of the said fingerprint identity window by predetermining a window-size for said fingerprint identity window and defining said dimensional area as from (XC - DIFF, YC - DIFF) to (XC + DIFF, YC + DIFF) where DIFF = ½ (window-size minus 1),

wherein (XC - DIFF) = Xs, (YC - DIFF) = Ys, (XC + DIFF) = Xe, and (YC + DIFF) = Ye.

88. A method as defined in Claim 82, further comprising the steps of:

selectively analyzing a plurality of different fingerprint pattern parts contained within said fingerprint identity window and computing a ridge count for each of said plurality of fingerprint pattern parts; and

compiling a data matrix comprised of a plurality of ridge counts computed for the said plurality of fingerprint pattern parts to provide a non-minutiae digitized numerical identifier indicative of said image of a fingerprint of a person to be identified.

89. A method as defined in Claim 88, further comprising: providing a non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data.

90. A method as defined in Claim 88, further comprising: providing a non-minutiae digitized numerical identifier having less than 100 bytes of fingerprint identification data.

91. A method as defined in Claim 88, further comprising: providing a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data.

92. A method as defined in Claim 83, further comprising: defining the dimensional area of the said fingerprint identity window by predetermining a window-size for said fingerprint identity window and defining said dimensional area as from (XC - DIFF, YC - DIFF) to (XC + DIFF, YC + DIFF) where DIFF = ½ (window-size minus 1) and (XC - DIFF) = Xs, (XC + DIFF) = Xe, (YC - DIFF) = Ys, and (YC + DIFF) = Ye.

93. A method as defined in Claim 92, further comprising the steps of:

computing a count S1 of ridges contained within a diagonal line from (Xs,Ys) to (Xe,Ye);

computing a count S2 of ridges contained within a diagonal line from (Xs,Ye) to (Xe,Ys);

computing a count Yma equal to the highest number of ridges found within any horizontal line in the Y-Axis "A-Range" which is defined as: Ys ≤ horizontal line < YC;

computing a count Ymb equal to the highest number of ridges found within any horizontal line in the Y-Axis "B-Range" which is defined as: YC < horizontal line ≤ Ye;

computing a count Ya equal to the sum total number of ridges found within all horizontal lines in the Y-Axis "A-Range" which is defined as: Ys ≤ horizontal line < YC, wherein Ya is stored as two counts, Yaα and Yaß, where Yaα = total number of base 256 ridges in said sum total, and Yaß = the remaining number or ridges counted which is always a number < 256, wherein Ya = (Yaα(256) + Yaß) + (window-size + 2);

computing a count Yb equal to the sum total number or ridges found within all horizontal lines in the Y-Axis "B-Range" which is defined as: YC < horizontal line ≤ Ye, wherein Yb is stored as two counts, Ybα and Ybß, where Ybα = total number of base 256 ridges in said sum total, and Ybß = the remaining number of ridges counted which is always a number < 256, wherein Yb = (Ybα(256) + Ybß) + (window-size ÷ 2);

computing a count Yc equal to the number of ridges found within horizontal line YC on the Y-axis, wherein Yc is a whole number and YC is the Y-axis center line of said fingerprint identity window;

computing a count Xma equal to the highest number of ridges found within any vertical line in the X-Axis "A-Range" which is defined as: Xs ≤ vertical line < XC;

computing a count Xmb equal to the highest number of ridges found within any vertical line in the X-Axis "B-Range" which is defined as: XC < vertical line ≤ Xe;

computing a count Xa equal to the sum total number of ridges found within all vertical lines in the X-Axis "A-Range" which is defined as: Xs ≤ vertical line < XC, wherein Xa is stored as two counts, Xaα and Xaß, where Xaα = total number of base 256 ridges in said sum total, and Xaß = the remaining number of ridges counted which is always a number < 256, wherein Xa = (Xaα(256) + Xaß) ÷ (window-size ÷ 2);

computing a count Xb equal to the sum total number of ridges found within all vertical lines in the X-Axis "B-Range" which is defined as: XC < vertical line ≤ Xe, wherein Xb is stored as two counts, Xbα and Xbß, where Xbα = total number of base 256 ridges in said sum total, and Xbß = the remaining number of ridges counted which is always a number < 256, wherein Xb = (Xbα(256) + Xbß) ÷ (window-size ÷ 2);

computing a count Xc equal to the number of ridges found within vertical line XC on the X-axis, wherein Xc is a whole number and XC is the X-axis center line of said fingerprint identity window; and

compiling a data matrix from said counts S1, S2, Yma, Ymb, Ya, Yb, Yc, Xma, Xmb, Xa, Xb and Xc to provide a non-minutiae digitized numeric identifier having 24 bytes of fingerprint identification data.

94. A method as defined in Claim 87, further comprising the steps of:

computing a count S1 of ridges contained within a diagonal line from (Xs,Ys) to (Xe,Ye);

computing a count S2 of ridges contained within a diagonal line from (Xs,Ye) to (Xe,Ys);

computing a count Yma equal to the highest number of ridges found within any horizontal line in the Y-Axis "A-Range" which is defined as: Ys ≤ horizontal line < YC;

computing a count Ymb equal to the highest number of ridges found within any horizontal line in the Y-Axis "B-Range" which is defined as: YC < horizontal line ≤ Ye;

computing a count Ya equal to the sum total number of ridges found within all horizontal lines in the Y-Axis "A-Range" which is defined as: Ys ≤ horizontal line < YC, wherein Ya is stored as two counts, Yaα and Yaß, where Yaα = total number of base 256 ridges in said sum total, and Yaß = the remaining number or ridges counted which is always a number < 256, wherein Ya = (Yaα(256) + Yaß) + (window-size + 2);

computing a count Yb equal to the sum total number or ridges found within all horizontal lines in the Y-Axis "B-Range" which is defined as: YC < horizontal line ≤ Ye, wherein Yb is stored as two counts, Ybα and Ybß, where Ybα = total number of base 256 ridges in said sum total, and Ybß = the remaining number of ridges counted which is always a number < 256, wherein Yb = (Ybα(256) + Ybß) + (window-size + 2);

computing a count Yc equal to the number or ridges found within horizontal line YC on the Y-axis, wherein Yc is a whole number and YC is the Y-axis center line of said fingerprint identity window;

computing a count Xma equal to the highest number or ridges found within any vertical line in the X-Axis "A-Range" which is defined as: Xs ≤ vertical line < XC;

computing a count Xmb equal to the highest number of ridges found within any vertical line in the X-Axis "B-Range" which is defined as: XC < vertical line ≤ Xe;

computing a count Xa equal to the sum total number of ridges found within all vertical lines in the X-Axis "A-Range" which is defined as: Xs ≤ vertical line < XC, wherein Xa is stored as two counts, Xaα and Xaß, where Xaα = total number of base 256 ridges in said sum total, and Xaß = the remaining number of ridges counted which is always a number < 256, wherein Xa = (Xaα(256) + Xaß) + (window-size + 2);

computing a count Xb equal to the sum total number of ridges found within all vertical lines in the X-Axis "B-Range" which is defined as: XC < vertical line ≤ Xe, wherein Xb is stored as two counts, Xbα and Xbß, where Xbα = total number of base 256 ridges in said sum total, and Xbß = the remaining number of ridges counted which is always a number < 256, wherein Xb = (Xbα(256) + Xbß) + (window-size + 2);

computing a count Xc equal to the number of ridges found within vertical line XC on the X-axis, wherein Xc is a whole number and XC is the X-axis center line of said fingerprint identity window; and

compiling a data matrix from said counts S1, S2, Yma, Ymb, Ya, Yb, Yc, Xma, Xmb, Xa, Xb and Xc to provide a non-minutiae digitized numeric identifier having 24 bytes of fingerprint identification data.

95. A method of verifying the identity of a person comprising the steps of:

a) obtaining an image of a fingerprint of a person to be identified provided via the use of an inkless means which when touched by a finger of said person causes immediate development of an image of the fingerprint of said finger in a black and white appearance;

b) providing a check payable to said person, having recorded therewith a non-minutiae numerical identifier which identifies the fingerprint of the said finger of said person;

c) reading said numerical identifier recorded on said check, and storing in memory the said numerical identifier;

d) video scanning said image of said fingerprint provided by said inkless means to produce image data and digitizing said

image data to produce a non-minutiae digitized numerical identifier indicative of said fingerprint; and

e) comparing the numerical identifier of the said check stored in memory with said non-minutiae digitized numerical identifier, to verify the identity of the said person.

96. A method as defined in Claim 95, further comprising as to step a) above: using the index finger of said person to be identified to provide said fingerprint.

97. A method as defined in Claim 95, further comprising as to step a) above: using the thumb of said person to be identified to provide said fingerprint.

98. A method as defined in Claim 95, further comprising as to step a) above: providing said image by using a toe of said person.

99. A method as defined in Claim 95, further comprising as to step d) above: using a video camera to video scan the said image of the said fingerprint provided on the said inkless means.

100. A method as defined in Claim 95, further comprising the step of: prior to digitizing the said image data, storing in a random-access memory means the said image data of the scanned fingerprint.

101. A method as defined in Claim 95, further comprising: displaying verification of the identity of said person.

102. A method as defined in Claim 101, further comprising: displaying non-verification of the identity of the said person.

103. A method as defined in Claim 102, further comprising: withholding said check upon occurrence of non-verification of the identity of said person.

104. A method for verifying the identity of a person comprising the steps of:

a) obtaining an image of a fingerprint of said person, said image being provided on an inkless means which when touched by a finger of the said person causes immediate development of an image of the fingerprint of said finger in a black and white appearance;

b) providing a check payable to said person, having recorded therewith an encrypted numerical identifier which identifies said fingerprint of the said person;

c) reading and decrypting said encrypted numerical identifier recorded on said check to provide a decrypted numerical identifier, and storing in memory said decrypted numerical identifier;

d) video scanning said image of said fingerprint to produce image data and digitizing said image data of the scanned fingerprint to produce a non-minutiae digitized numerical identifier indicative of said fingerprint; and

e) comparing said non-minutiae digitized numerical identifier with said decrypted numerical identifier, to verify the identity of said person.

105. A method as defined in Claim 104, further comprising as to step a) above: using the index finger of said person to be identified to provide said fingerprint.

106. A method as defined in Claim 104, further comprising as to step a) above: using the thumb of said person to be identified to provide said fingerprint.

107. A method as defined in Claim 104, further comprising as to step a) above: providing said image by using a toe of said person.

108. A method as defined in Claim 104, further comprising as to step d) above: using a video camera to video scan the said image of the said fingerprint provided on the said inkless means.

109. A method as defined in Claim 104, further comprising the step of: prior to digitizing the said image data, storing in a random-access memory means the said image data of the scanned fingerprint.

110. A method as defined in Claim 104, further comprising: displaying verification of the identity of said person.

111. A method as defined in Claim 110, further comprising: displaying non-verification of the identity of the said person.

112. A method as defined in Claim 111, further comprising: withholding said check upon occurrence of non-verification of the identity of said person.

113. A method as defined in Claim 104, wherein said decrypted numerical identifier and said non-minutiae numerical identifier each have less than 400 bytes of fingerprint identification data.

114. A method as defined in Claim 104, wherein said decrypted numerical identifier and said non-minutiae numerical identifier each have 24 bytes of fingerprint identification data.

115. A method as defined in Claim 95, wherein said non-minutiae numerical identifier and said non-minutiae digitized numerical identifier each have less than 400 bytes of fingerprint identification data.

116. A method as defined in Claim 95, wherein said non-minutiae numerical identifier and said non-minutiae digitized numerical identifier each have 24 bytes of fingerprint identification data.

117. A method as defined in Claim 28, wherein said numerical identifier recorded within said portable personnel identification means and said non-minutiae digitized numerical identifier each have less than 400 bytes of fingerprint identification data.

118. A method as defined in Claim 31, wherein said numerical identifier recorded within said credit card and said non-minutiae digitized numerical identifier each have 24 bytes of fingerprint identification data.

119. A method as defined in Claim 50, wherein said decrypted numerical identifier and said non-minutiae digitized numerical identifier each have less than 400 bytes of fingerprint identification data.

120. A method as defined in Claim 54, wherein said decrypted numerical identifier and said non-minutiae digitized numerical identifier each have 24 bytes of fingerprint identification data.

121. A method as defined in Claim 1, further comprising as to step c: providing the said non-minutiae digitized numerical identifier to another for recording said identifier within said identification means.

122. A method as defined in Claim 41, further comprising as to step c: providing said encrypted digitized numerical identifier to another for recording said encrypted identifier within said identification means.

123. A method as defined in Claim 10, further comprising as to step c: providing the said non-minutiae digitized numerical identifier to another for recording said identifier within said identification means.

124. A method as defined in Claim 19, further comprising as to step c: providing said encrypted digitized numerical identifier to another for recording said encrypted identifier within said identification means.

125. A method of verifying the identity of a check payee comprising the steps of:

a) obtaining an image of a fingerprint of a person to be identified as a check payee, said image being provided via the use of an inkless means which when touched by a finger of said person causes immediate development of an image of the fingerprint of said finger in a black and white appearance;

b) providing a check payable to said check payee;

c) providing a portable personnel identification means having recorded therewith a non-minutiae numerical identifier which identifies the fingerprint of said check payee;

d) reading said numerical identifier recorded on said portable personnel identification means, and storing in memory the said numerical identifier;

e) video scanning said image of said fingerprint provided by said inkless means to produce image data and digitizing said image data to produce a non-minutiae digitized numerical identifier indicative of said fingerprint;

f) comparing the numerical identifier of the said portable personnel identification means stored in memory with said non-minutiae digitized numerical identifier, to verify the identity of said person as the said check payee; and

g) printing on said check payable an identity verification message.

126. A method as defined in Claim 125, further comprising as to step a) above: using the index finger of said person to be identified to provide said fingerprint.

127. A method as defined in Claim 125, further comprising as to step a) above: using the thumb of said person to be identified to provide said fingerprint.

128. A method as defined in Claim 125, further comprising as to step a) above: providing said image by using a toe of said person.

129. A method as defined in Claim 125, further comprising as to step d) above: using a video camera to video scan the said image of the said fingerprint provided on the said inkless means.

130. A method as defined in Claim 125, further comprising the step of: prior to digitizing the said image data, storing in a random-access memory means the said image data of the scanned fingerprint.

131. A method for verifying the identity of a check payee comprising the steps of:

a) obtaining an image of a fingerprint of a person to be identified as a check payee, said image being provided on an inkless means which when touched by a finger of the said person causes immediate development of an image

of the fingerprint of said finger in a black and white appearance;

b) providing a check payable to said check payee;

c) providing a portable personnel identification means having recorded therewith an encrypted non-minutiae numerical identifier which identifies the fingerprint of said check payee;

d) reading and decrypting said encrypted numerical identifier recorded on said portable personnel identification means to provide a decrypted numerical identifier, and storing in memory said decrypted numerical identifier;

e) video scanning said image of said fingerprint to produce image data and digitizing said image data of the scanned fingerprint to produce a non-minutiae digitized numerical identifier indicative of said fingerprint;

f) comparing said non-minutiae digitized numerical identifier with said decrypted numerical identifier, to verify the identity of said person as the said check payee; and

g) printing on said check payable an identification verification message.

132. A method as defined in Claim 131, further comprising as to step a) above: using the index finger of said person to be identified to provide said fingerprint.

133. A method as defined in Claim 131, further comprising as to step a) above: using the thumb of said person to be identified to provide said fingerprint.

134. A method as defined in Claim 131, further comprising as to step a) above: providing said image by using a toe of said person.

135. A method as defined in Claim 131, further comprising as to step d) above: using a video camera to video scan the said image of the said fingerprint provided on the said inkless means.

136. A method as defined in Claim 131, further comprising the step of: prior to digitizing the said image data, storing in a random-access memory means the said image data of the scanned fingerprint.

137. A method as defined in Claim 125, wherein said non-minutiae numerical identifier and said non-minutiae digitized numerical identifier each have less than 400 bytes of fingerprint identification data.

138. A method as defined in Claim 125, wherein said non-minutiae numerical identifier and said non-minutiae digitized numerical identifier each have 24 bytes of fingerprint identification data.

139. A method as defined in Claim 131, wherein said decrypted numerical identifier and said non-minutiae digitized numerical identifier each have less than 400 bytes of fingerprint identification data.

140. A method as defined in Claim 131, wherein said decrypted numerical identifier and said non-minutiae digitized numerical identifier each have 24 bytes of fingerprint identification data.

141. An automatic non-minutiae fingerprint identification system comprising in combination:

fingerprint format holder means for positioning a fingerprint format in a predetermined scan position;

video scanner means for scanning an image of a fingerprint of a person to be identified provided by said fingerprint format, to produce image data including fingerprint image data and whitespace data;

video digitizer means for converting said fingerprint image and whitespace data into digital image data;

addressable memory means for storing said digital image data;

program-controlled processor means for selectively analyzing a plurality of different fingerprint pattern parts of the said digital image data stored in said addressable memory means, to provide a non-minutiae digitized numerical identifier indicative of said image of a fingerprint of a person to be identified;

portable personnel identification card reader means for reading a numerical identifier recorded within the confines of a portable personnel identification card means and indicative of said fingerprint of said person to be identified;

memory means for storing said numerical identifier read by said card reader means; and

means for comparing the said numerical identifier with said non-minutiae digitized numerical identifier, to verify the identity of the said person to be identified.

142. A system as defined in Claim 141 further comprising: means for defining a fingerprint identity window within the said digital image data.

143. A system as defined in Claim 141 further comprising: means for image framing the said digital image data to a predetermined dimension and for determining the location of the said fingerprint image data within the said digital image data.

144. A system as defined in Claim 141 further comprising LCD display means for displaying system messages.

145. A system as defined in Claim 144 wherein said program-controlled processor means provides a non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data.

146. A system as defined in Claim 144 wherein said program-controlled processor means provides a non-minutiae digitized numerical identifier having less than 100 bytes of fingerprint identification data.

147. A system as defined in Claim 144 wherein said program-controlled processor means provides a non-minutiae digitized numerical identifier having 24 bytes of fingerprint identification data.

148. A system as defined in Claim 144 further comprising: inkless fingerprint format means for providing said image of a fingerprint.

149. A system as defined in Claim 142 further comprising: inkless fingerprint format means for providing said image of a fingerprint.

150. A system as defined in Claim 143 further comprising: inkless fingerprint format means for providing said image of a fingerprint.

151. A system as defined in Claim 144 further comprising: wherein said portable personnel identification card reader means comprises a smart card reader.

152. A system as defined in Claim 151 wherein said program-controlled processor means provides a non-minutiae digitized numerical identifier having less than 400 bytes of fingerprint identification data.

153. A system as defined in Claim 151 further comprising inkless fingerprint format means for providing said image of a fingerprint.

154. A system as defined in Claim 141 further comprising: printer means for printing on a check payable an identity verification message.

155. A system as defined in Claim 154 further comprising check payable entry and exit slots which function to provide access to and exit from said printer means of said check payable.

156. A system as defined in Claim 151 further comprising slot access means for inserting a smart card into said smart card reader.

157. A system as defined in Claim 141 further comprising: inkless fingerprint format means for providing said image of a fingerprint.

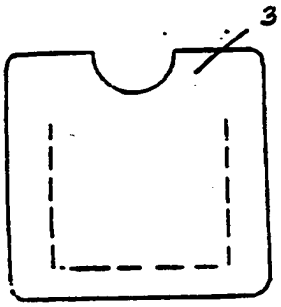


FIG. 1b

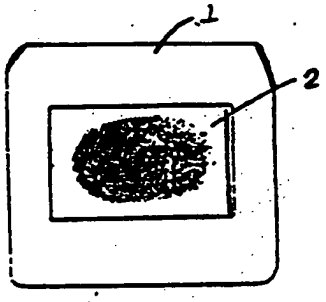


FIG. 1a

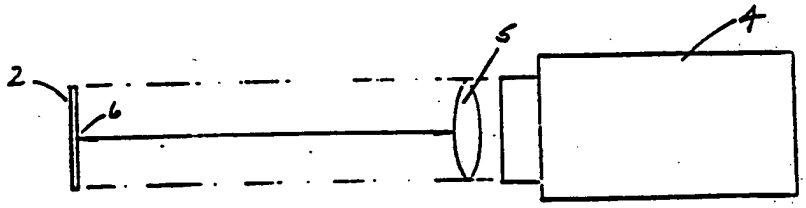


FIG. 2

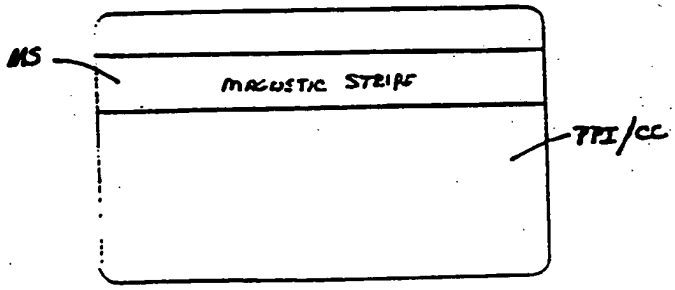
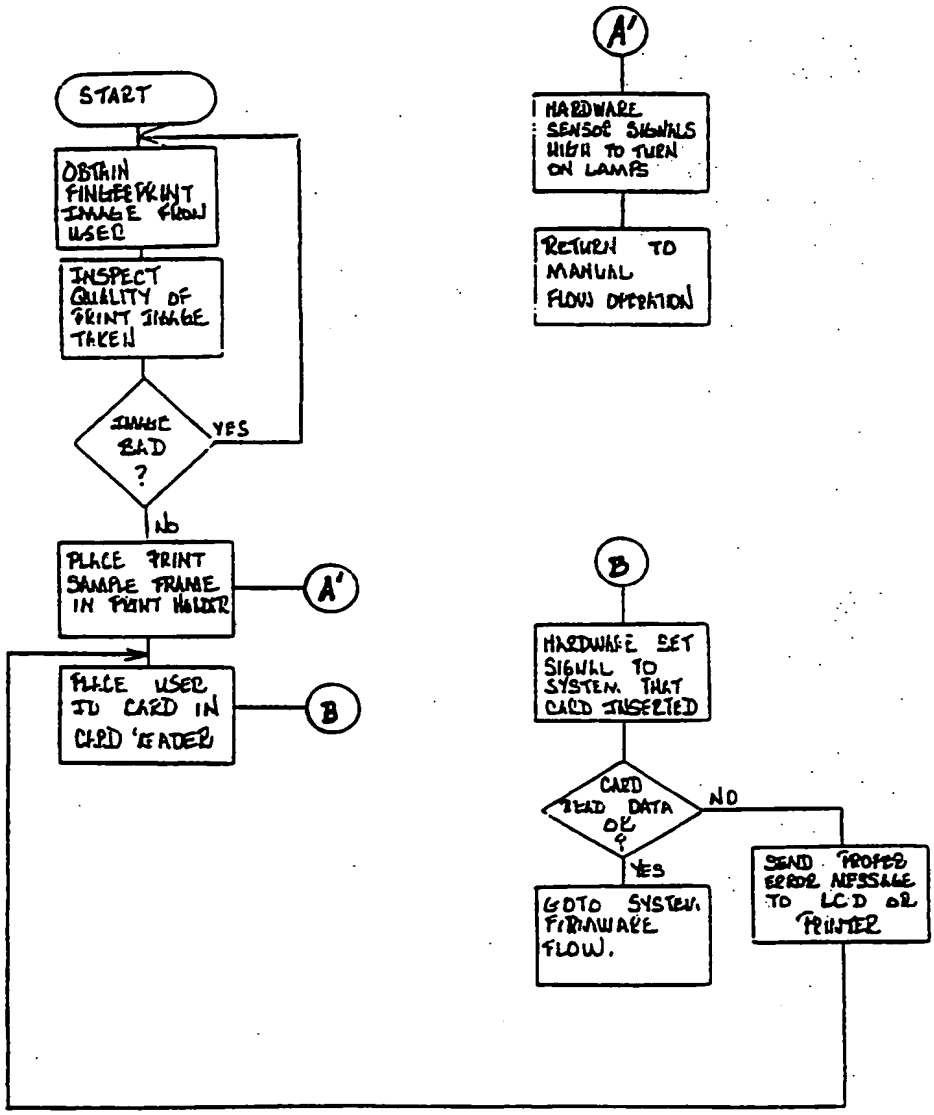


FIG. 3



SYSTEM MANUAL & HARDWARE FLOW

FIG. 4

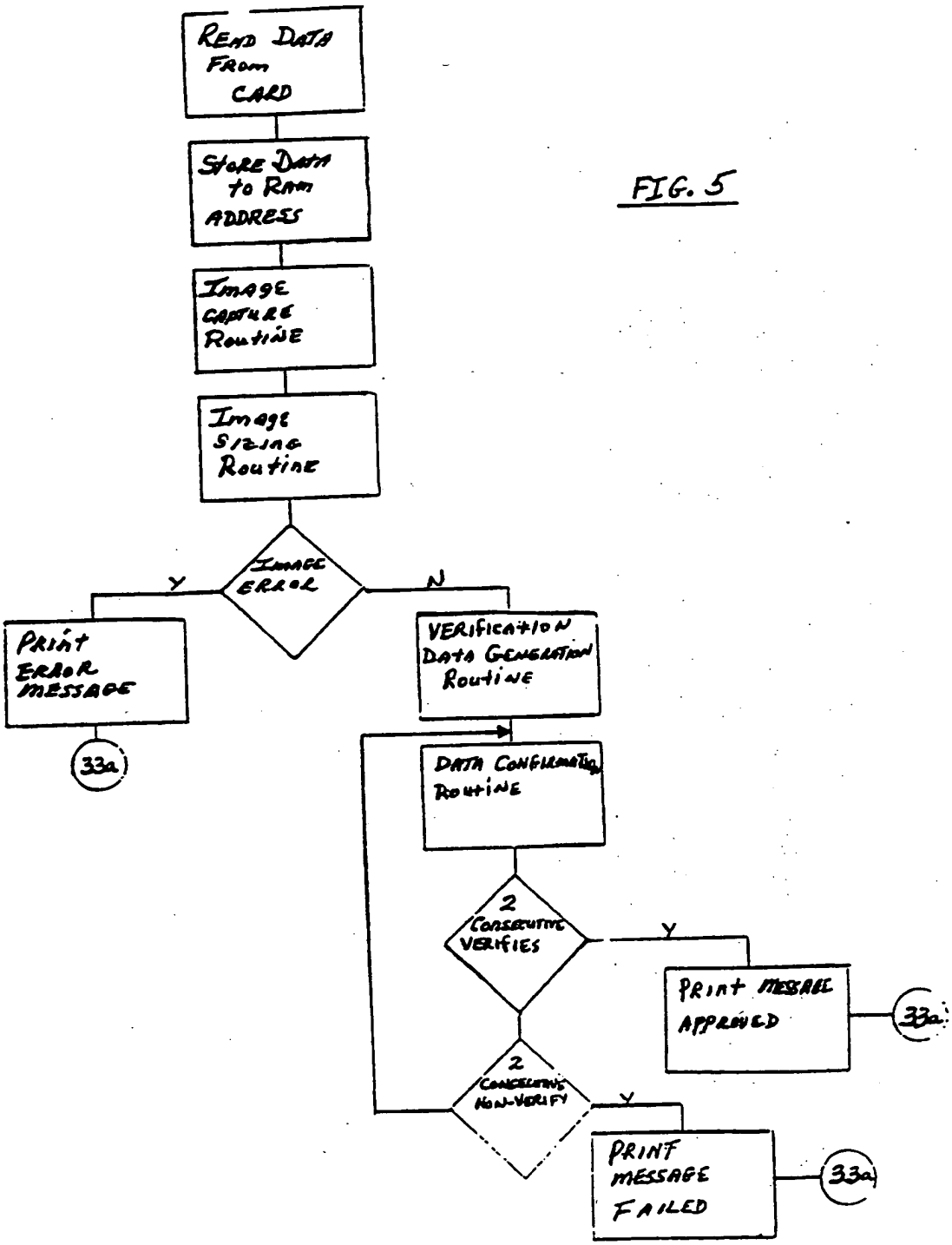

READ DATA FROM CARD
STORE DATA to RAM ADDRESS
IMAGE CAPTURE Routine
Image Sizing Routine
IMAGE ERROR
Y
N
PRINT ERROR MESSAGE
33a
VERIFICATION DATA GENERATION Routine
DATA CONFIRMATION Routine
2 CONSECUTIVE VERIFIES
Y
PRINT MESSAGE APPROVED
33a
2 CONSECUTIVE NON-VERIFY
Y
PRINT MESSAGE FAILED
33a

FIG. 5

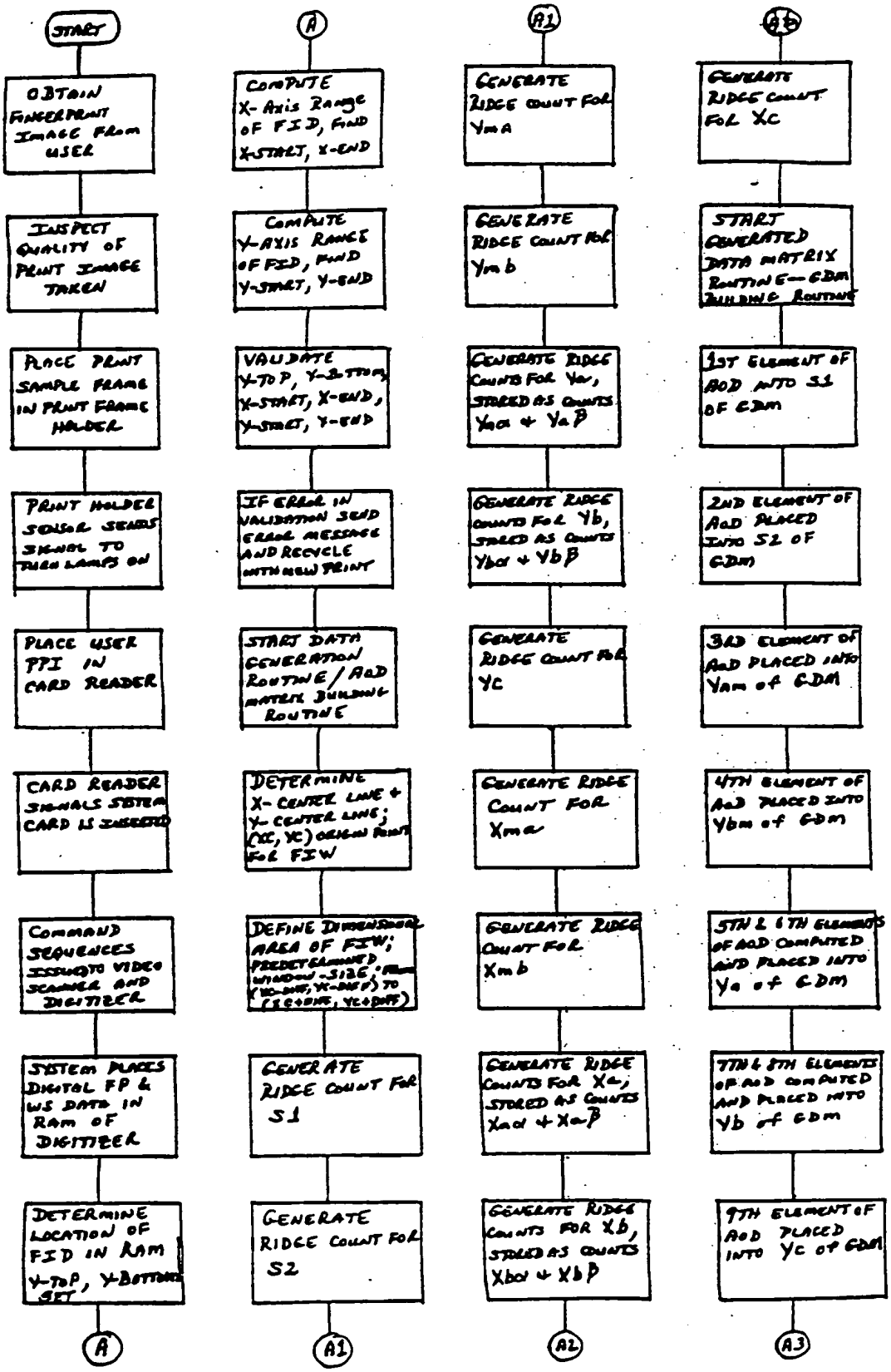

START
OBTAIN FINGERPRINT IMAGE FROM USER
INSPECT QUALITY OF PRINT IMAGE TAKEN
PLACE PRINT SAMPLE FRAME IN PRINT FRAME HOLDER
PRINT HOLDER SENSOR SENDS SIGNAL TO TURN LAMPS ON
PLACE USER PPI IN CARD READER
CARD READER SIGNALS SYSTEM CARD IS INSERTED
COMMAND SEQUENCES ISSUED TO VIDEO SCANNER AND DIGITIZER
SYSTEM PLACES DIGITAL FP & WS DATA IN RAM OF DIGITIZER
DETERMINE LOCATION OF FID IN RAM Y-TOP, Y-BOTTOM SET
A
COMPUTE X-AXIS RANGE OF FID, FIND X-START, X-END
COMPUTE Y-AXIS RANGE OF FID, FIND Y-START, Y-END
VALIDATE Y-TOP, Y-BOTTOM, X-START, X-END, Y-START, Y-END
IF ERROR IN VALIDATION SEND ERROR MESSAGE AND RECYCLE WITH NEW PRINT
START DATA GENERATION ROUTINE / ADD MATRIX BUILDING ROUTINE
DETERMINE X-CENTER LINE + Y-CENTER LINE; (XC, YC) ORIGIN POINT FOR FIW
DEFINE DIMENSIONAL AREA OF FIW; PREDETERMINED WINDOW = 512, FROM (XC-DIFF, YC-DIFF) TO (XC+DIFF, YC+DIFF)
GENERATE RIDGE COUNT FOR S1
GENERATE RIDGE COUNT FOR S2
A1
GENERATE RIDGE COUNT FOR YmA
GENERATE RIDGE COUNT FOR Ymb
GENERATE RIDGE COUNTS FOR Ya, STORED AS COUNTS Yaα + YaβP
GENERATE RIDGE COUNTS FOR Yb, STORED AS COUNTS Ybα + YbβP
GENERATE RIDGE COUNT FOR Yc
GENERATE RIDGE COUNT FOR Xma
GENERATE RIDGE COUNT FOR Xmb
GENERATE RIDGE COUNTS FOR Xa, STORED AS COUNTS Xaα + XaβP
GENERATE RIDGE COUNTS FOR Xb, STORED AS COUNTS Xbα + XbβP
A2
A3
GENERATE RIDGE COUNT FOR Xc
START GENERATED DATA MATRIX ROUTINE — GDM BUILDING ROUTINE
1ST ELEMENT OF AOD INTO S1 OF GDM
2ND ELEMENT OF AOD PLACED INTO S2 OF GDM
3RD ELEMENT OF AOD PLACED INTO Yam of GDM
4TH ELEMENT OF AOD PLACED INTO Ybm of GDM
5TH & 6TH ELEMENTS OF AOD COMPUTED AND PLACED INTO Ya of GDM
7TH & 8TH ELEMENTS OF AOD COMPUTED AND PLACED INTO Yb of GDM
9TH ELEMENT OF AOD PLACED INTO Yc OF GDM

FIG. 6a

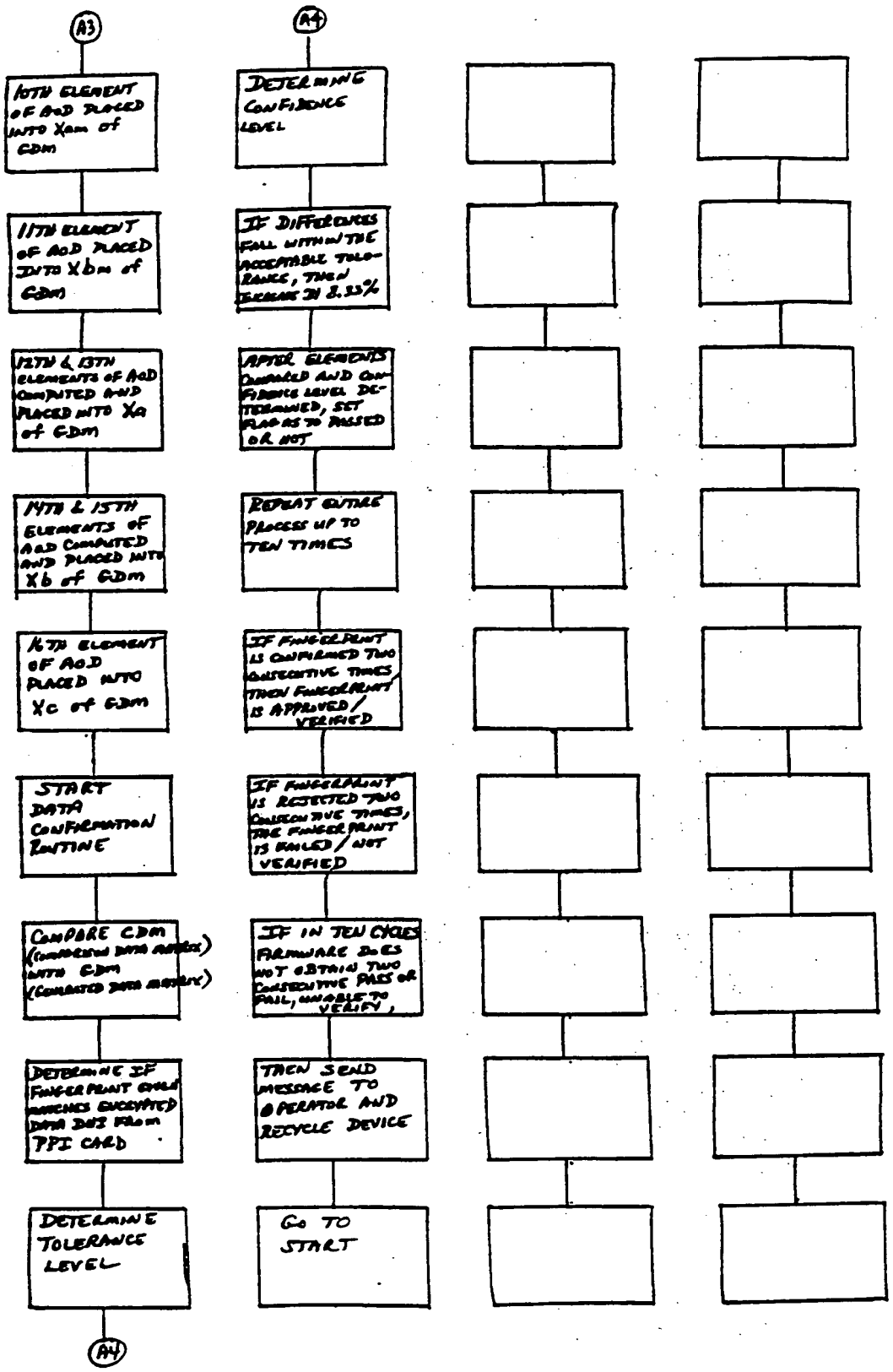

A3
10TH ELEMENT OF AOD PLACED INTO Xam of GDm
11TH ELEMENT OF AOD PLACED INTO Xbm of GDm
12TH & 13TH ELEMENTS OF AOD COMPUTED AND PLACED INTO Xa of GDm
14TH & 15TH ELEMENTS OF AOD COMPUTED AND PLACED INTO Xb of GDm
16TH ELEMENT OF AOD PLACED INTO Xc of GDm
START DATA CONFIRMATION ROUTINE
COMPARE CDm (CONFIDENCE DATA MATRIX) INTO GDm (COMBINED DATA MATRIX)
DETERMINE IF FINGERPRINT DATA MATCHES ENCRYPTED DATA DATA FROM PPI CARD
DETERMINE TOLERANCE LEVEL
A4
A4
DETERMINE CONFIDENCE LEVEL
IF DIFFERENCES FALL WITHIN THE ACCEPTABLE TOLERANCE, THEN TOLERANCE IS 2.33%
AFTER ELEMENTS COMPARED AND CONFIDENCE LEVEL DETERMINED, SET FLAG AS TO PASSED OR NOT
REPEAT ENTIRE PROCESS UP TO TEN TIMES
IF FINGERPRINT IS CONFIRMED TWO CONSECUTIVE TIMES, THEN FINGERPRINT IS APPROVED / VERIFIED
IF FINGERPRINT IS REJECTED TWO CONSECUTIVE TIMES, THE FINGERPRINT IS FAILED / NOT VERIFIED
IF IN TEN CYCLES FIRMWARE DOES NOT OBTAIN TWO CONSECUTIVE PASS OR FAIL, UNABLE TO VERIFY,
THEN SEND MESSAGE TO OPERATOR AND RECYCLE DEVICE
GO TO START

FIG. 6b

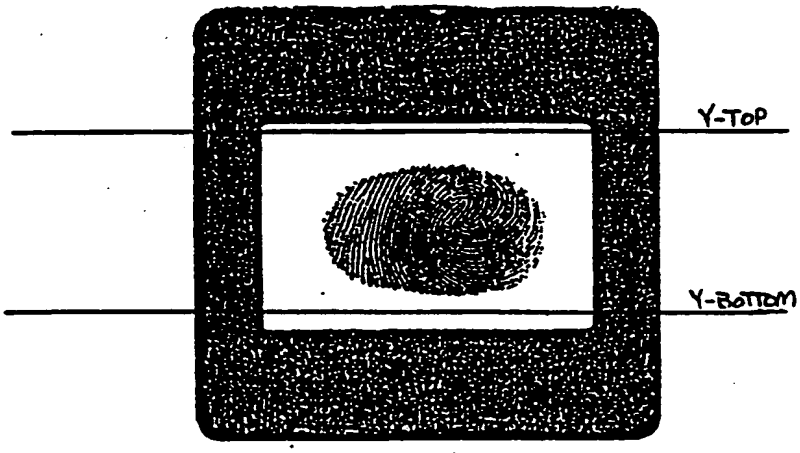

Y-TOP
Y-BOTTOM

FIG. 7a

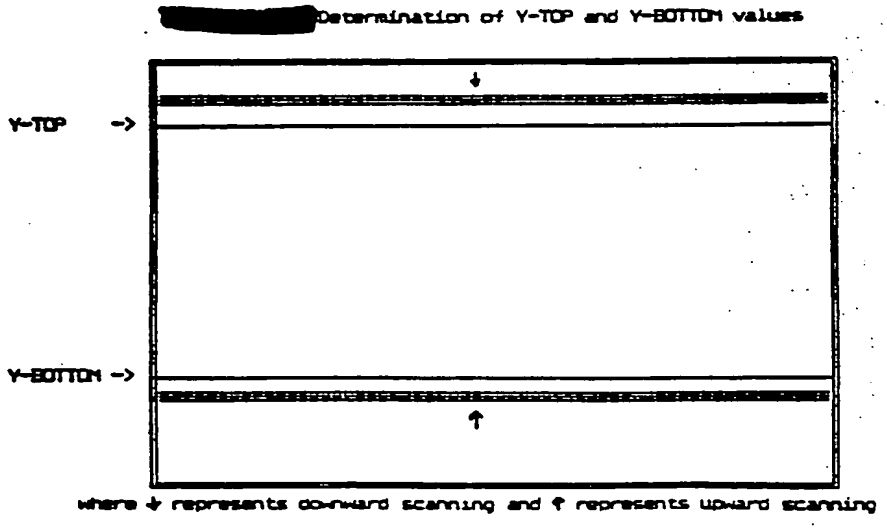

Determination of Y-TOP and Y-BOTTOM values
Y-TOP ->
Y-BOTTOM ->
where ↓ represents downward scanning and ↑ represents upward scanning

FIG. 7b

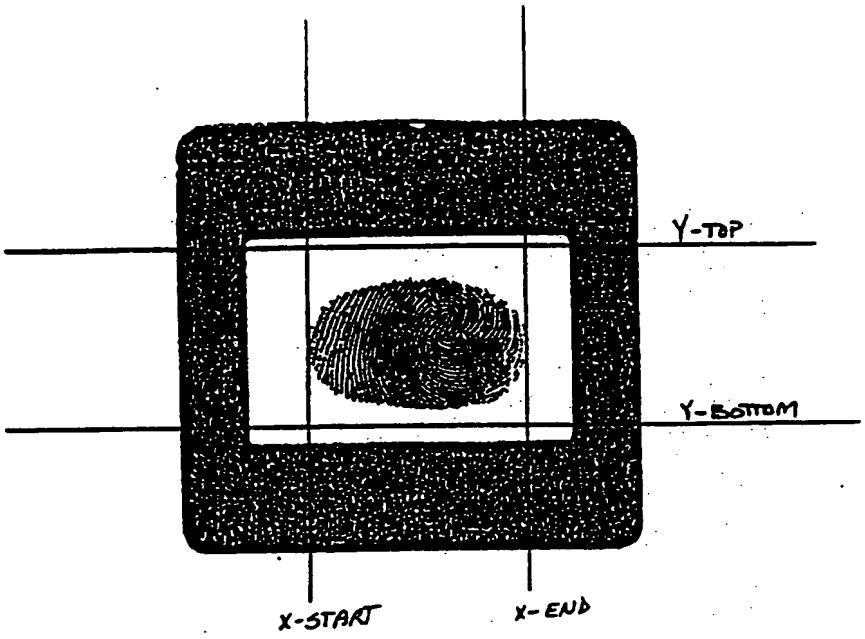

Y-TOP
Y-BOTTOM
X-START
X-END

FIG. 8a

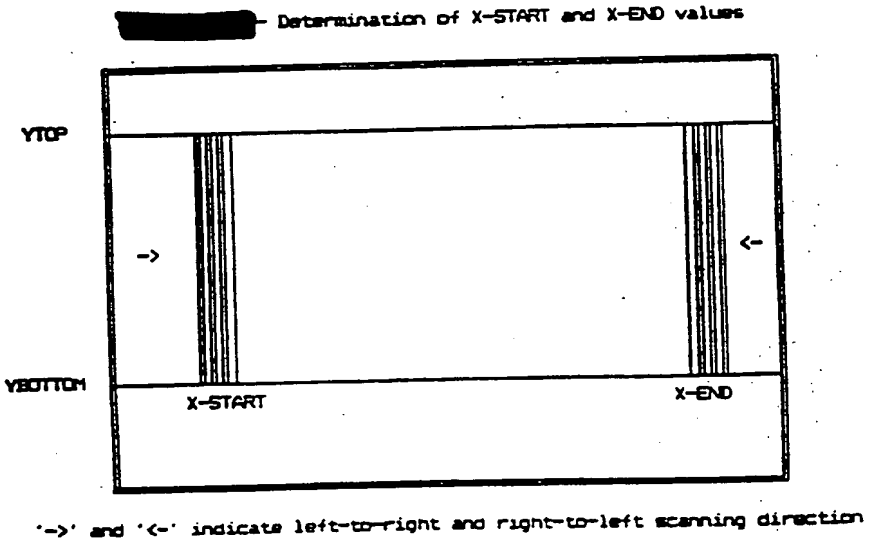

Determination of X-START and X-END values
YTOP
YBOTTOM
->
<-
X-START
X-END
'->' and '<-' indicate left-to-right and right-to-left scanning direction

FIG. 8b

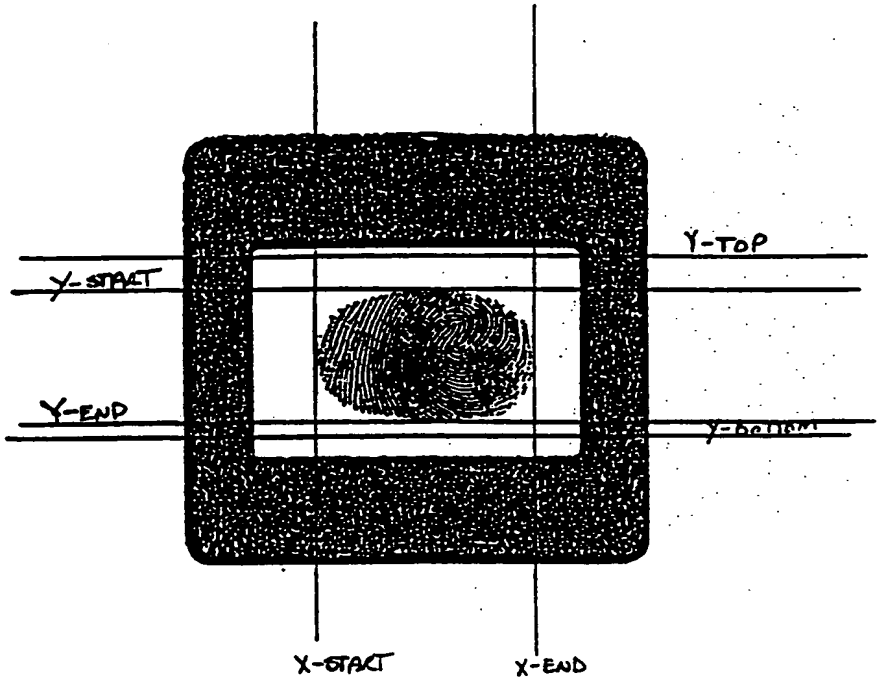

Y-TOP
Y-START
Y-END
Y-BOTTOM
X-START
X-END

FIG. 9a

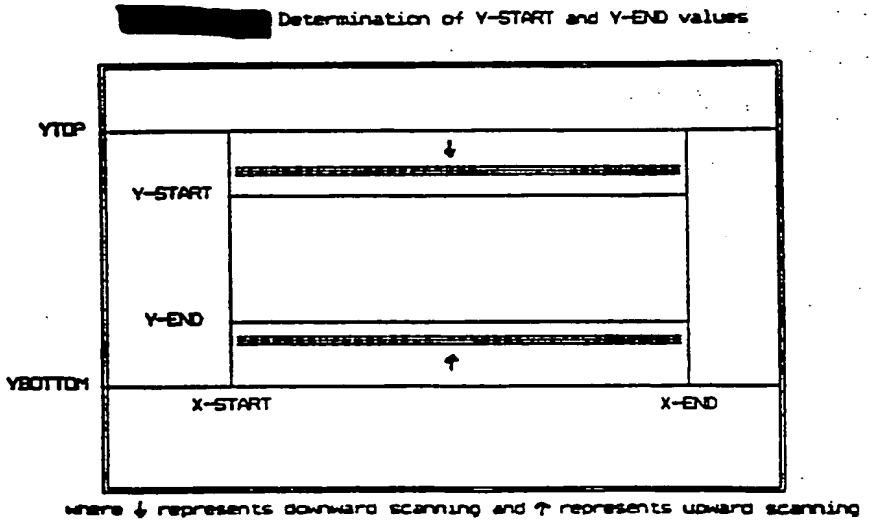

Determination of Y-START and Y-END values
YTOP
Y-START
Y-END
YBOTTOM
X-START
X-END
where ↓ represents downward scanning and ↑ represents upward scanning

FIG. 9b

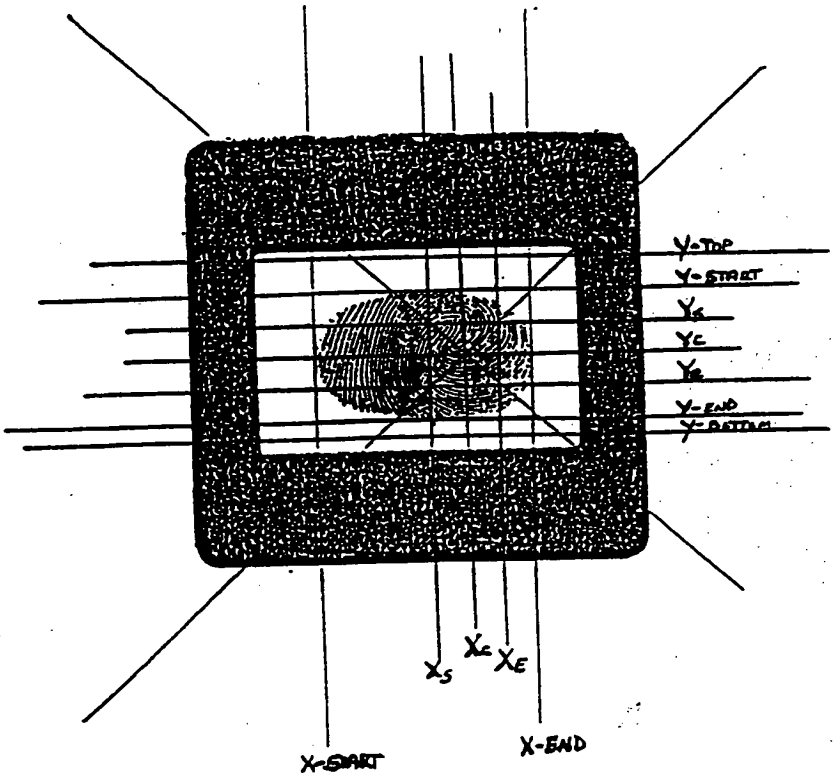


FIG. 10a

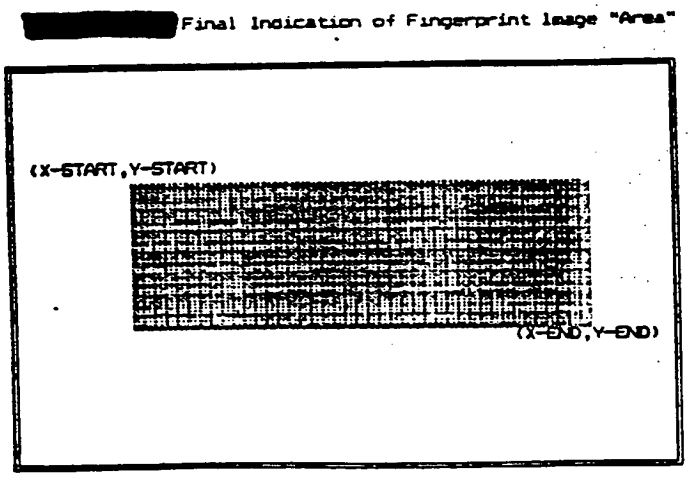


FIG. 10b

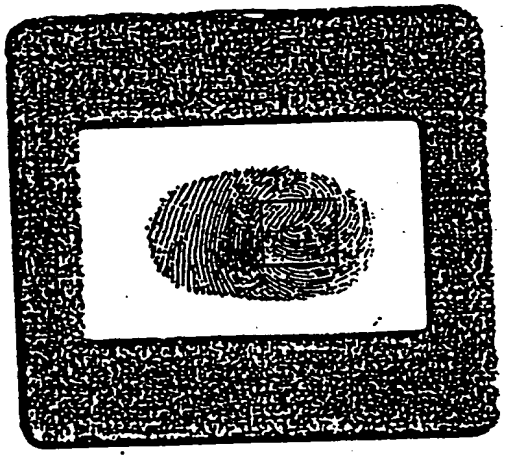


FIG. 11a

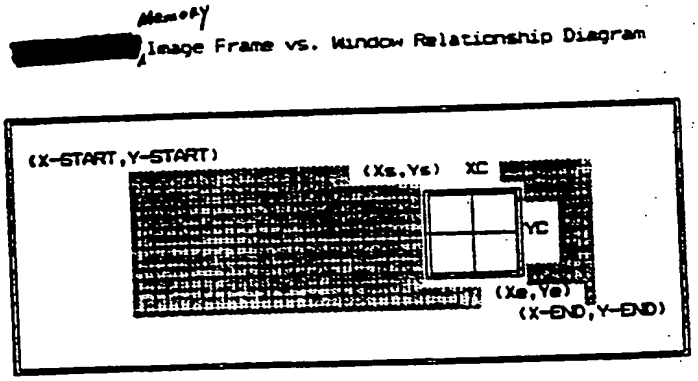


FIG. 11b

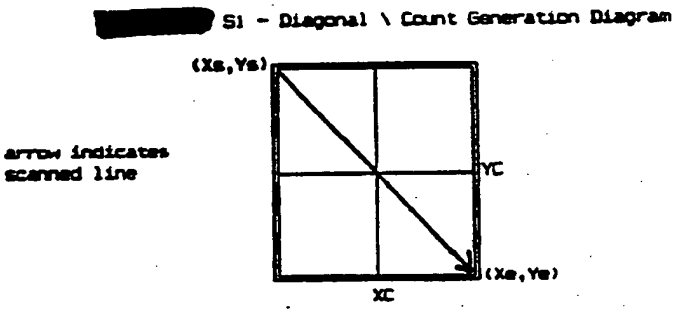

S1 - Diagonal \ Count Generation Diagram
(Xs,Ys)
arrow indicates scanned line
YC
(Xe,Ye)
XC

FIG. 12

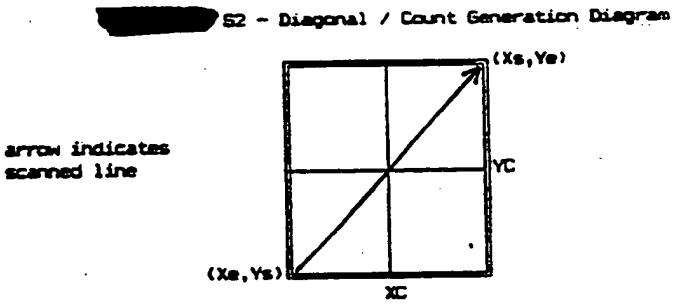

S2 - Diagonal / Count Generation Diagram
(Xs,Ye)
arrow indicates scanned line
YC
(Xe,Ys)
XC

FIG. 13

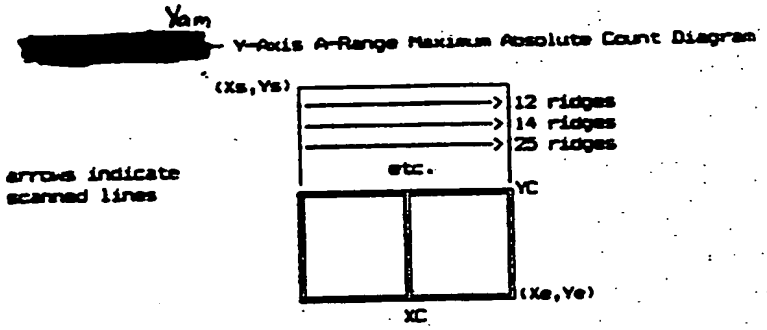

Yam
[redacted] - Y-Axis A-Range Maximum Absolute Count Diagram
(Xs,Ys)
12 ridges
14 ridges
25 ridges
etc.
arrows indicate scanned lines
YC
(Xe,Ye)
XC

FIG. 14

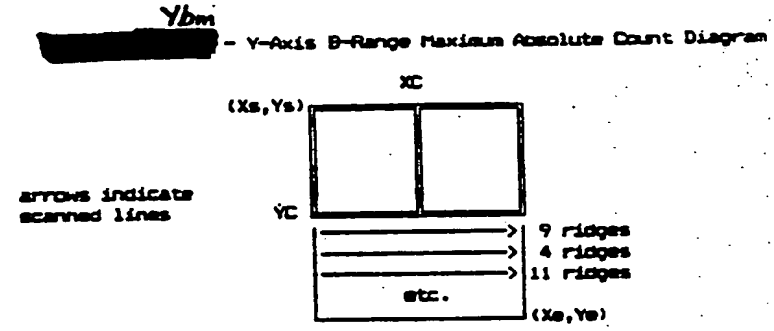

Ybm
[redacted] - Y-Axis B-Range Maximum Absolute Count Diagram
XC
(Xs,Ys)
arrows indicate scanned lines
YC
9 ridges
4 ridges
11 ridges
etc.
(Xe,Ye)

FIG. 15

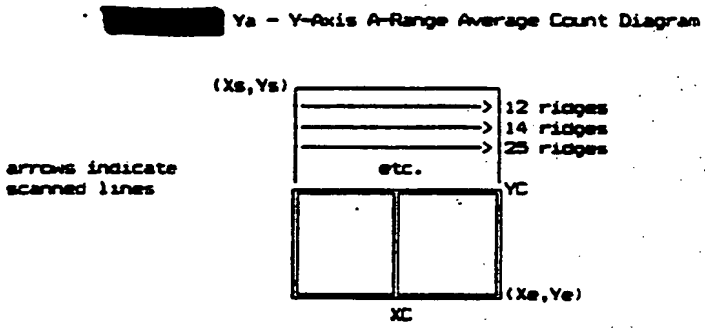

[redacted] Ya - Y-Axis A-Range Average Count Diagram
(Xs,Ys)
12 ridges
14 ridges
25 ridges
etc.
arrows indicate scanned lines
YC
(Xe,Ye)
XC

FIG. 16

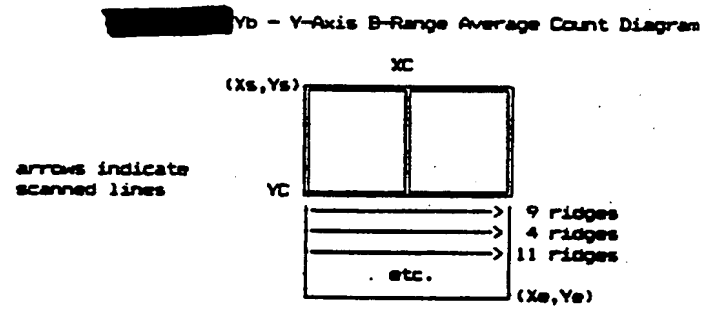

[redacted] Yb - Y-Axis B-Range Average Count Diagram
XC
(Xs,Ys)
arrows indicate scanned lines
YC
9 ridges
4 ridges
11 ridges
etc.
(Xe,Ye)

FIG. 17

[redacted] Yc - Y-Axis Center Line Absolute Count Diagram

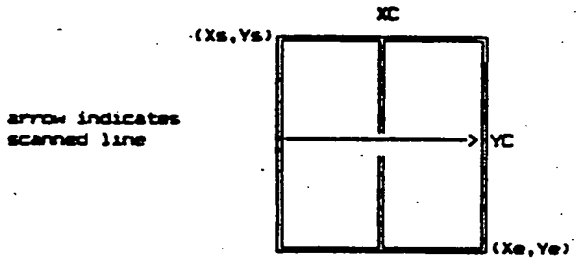


FIG. 18

Xam

[redacted] X-Axis A-Range Maximum Absolute Count Diagram

9 10 11 (ridges found on each vertical line)

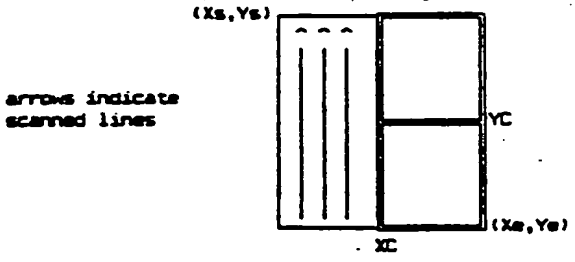


FIG. 19

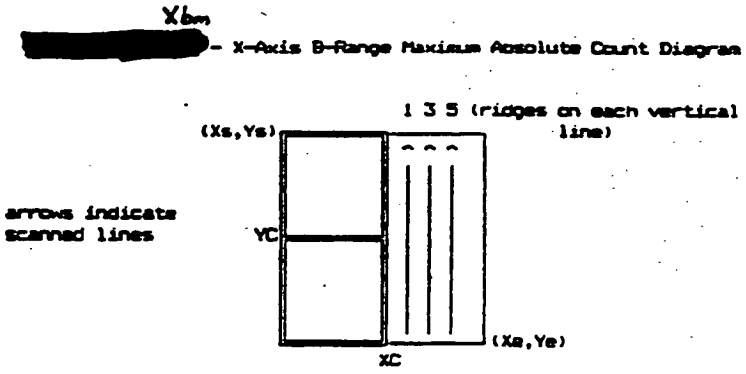

Xbm
[redacted] - X-Axis B-Range Maximum Absolute Count Diagram
1 3 5 (ridges on each vertical line)
(Xs,Ys)
arrows indicate scanned lines
YC
(Xe,Ye)
XC

FIG. 20

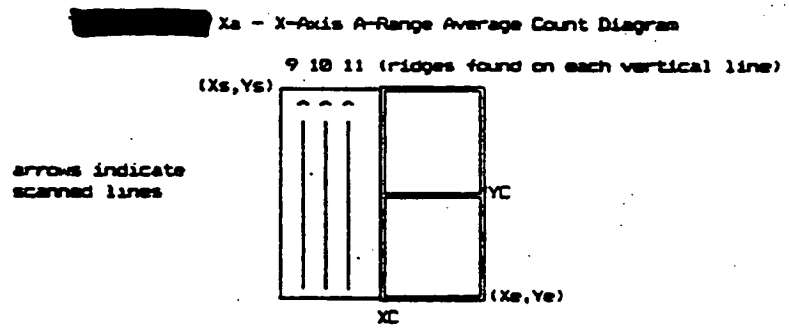

[redacted] Xa - X-Axis A-Range Average Count Diagram
9 10 11 (ridges found on each vertical line)
(Xs,Ys)
arrows indicate scanned lines
YC
(Xe,Ye)
XC

FIG. 21

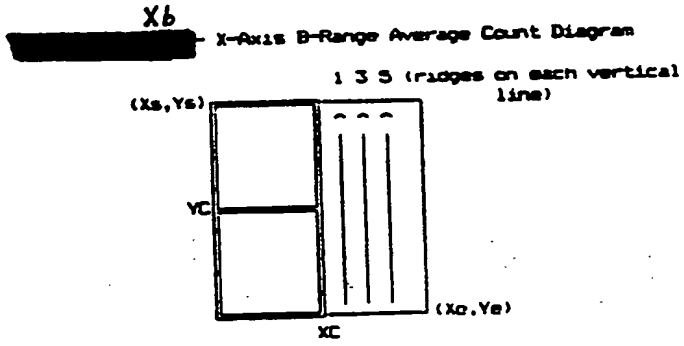

Xb
[redacted] X-Axis B-Range Average Count Diagram
1 3 5 (ridges on each vertical line)
(Xs,Ys)
YC
(Xe,Ye)
XC

FIG. 22

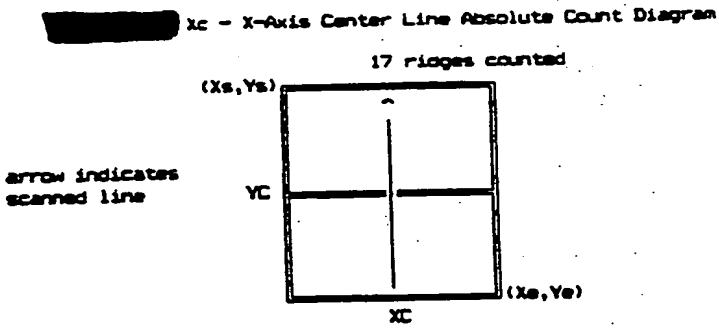

[redacted] Xc - X-Axis Center Line Absolute Count Diagram
17 ridges counted
(Xs,Ys)
arrow indicates scanned line
YC
(Xe,Ye)
XC

FIG. 23

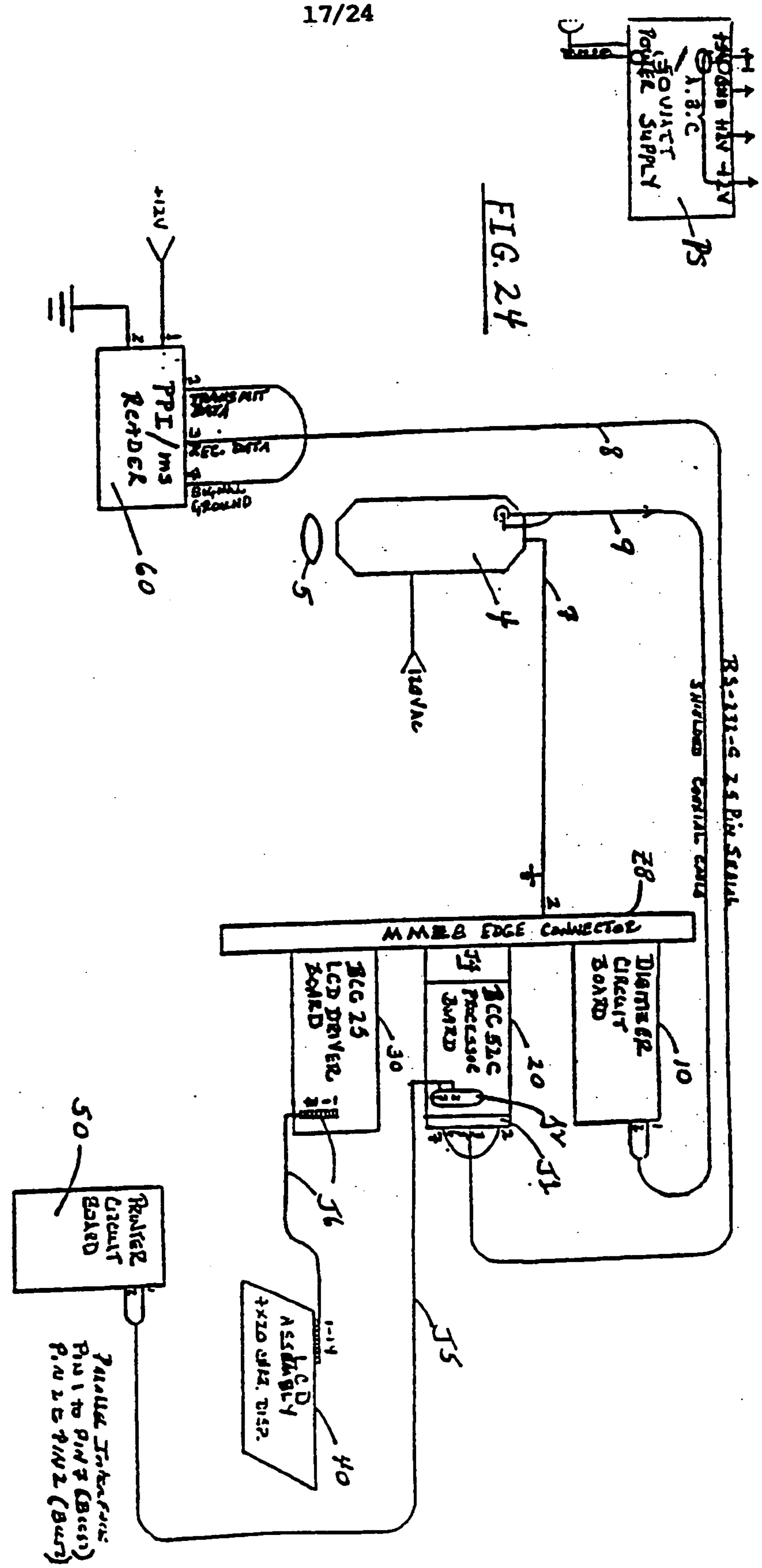

MMEB EDGE CONNECTOR
DIMMER CIRCUIT BOARD
PRINTER CIRCUIT BOARD
LCD DRIVER BOARD
PROCESSOR BOARD
LCD ASSEMBLY
POWER SUPPLY
RS-232-C 25 PIN SERIAL
SHIELDED CONTROL CABLE

FIG. 24

System Bus Pinout

PIN	SIGNAL MM28	DESCRIPTION	DIGITIZER
1	+5	+5 Volt Power Input	+5
2	GND	Signal Ground	GND
3	N/C	No Connection	N/C
4	AD3	Multiplexed Address/Data	AD3
5	AD4	Multiplexed Address/Data	AD4
6	AD5	Multiplexed Address/Data	AD5
7	AD6	Multiplexed Address/Data	AD6
8	AD7	Multiplexed Address/Data	AD7
9	AD0	Multiplexed Address/Data	AD0
10	AD1	Multiplexed Address/Data	AD1
11	AD2	Multiplexed Address/Data	AD2
12	P2/0	Port 2 Bit 0	P2/0
13	P2/1	Port 2 Bit 1	P2/1
14	P2/2	Port 2 Bit 2	P2/2
15	P2/3	Port 2 Bit 3	P2/3
16	P2/4	Port 2 Bit 4	P2/4
17	P2/5	Port 2 Bit 5	P2/5
18	P2/6	Port 2 Bit 6	P2/6
19	P2/7	Port 2 Bit 7	P2/7
20	R/W	Read/Write	R/W
21	DS	Data Strobe	DS
22	AS	Address Strobe	AS
A	-12	-12 Volt Power Input	-12
B	+12	+12 Volt Power Input	+12
C	N/C	No Connection	N/C
D	N/C	No Connection	N/C
E	P3/1	Port 3 Bit 1	P3/1
F	N/C	No Connection	N/C
H	P3/2	Port 3 Bit 2	P3/2
J	N/C	No Connection	N/C
K	P3/5	Port 3 Bit 5	P3/5
L	P3/6	Port 3 Bit 6	P3/6
M	P3/7	Port 3 Bit 7	P3/7
N	P3/0	Port 3 Bit 0	P3/0
P	P3/4	Port 3 Bit 4	P3/4
R	P3/3	Port 3 Bit 3	P3/3
S	A15	Address Bus	A15
T	A14	Address Bus	A14
U	A13	Address Bus	A13
V	A12	Address Bus	A12
W	A11	Address Bus	A11
X	A10	Address Bus	A10
Y	A9	Address Bus	A9
Z	A8	Address Bus	A8

FIG. 25

J4

MMZ8 Bus Pin Configuration
(End View - Edge Card Connector)

Component Side			Solder Side
- 12 Volts ---------->	A	1	<-------- +5 Volts
+ 12 Volts ---------->	B	2	<-------- Ground
Reset ---------->	C	3	<-------- No Connection
No Connection ------->	D	4	<-------- Address/Data 3
Timer Zero Input --->	E	5	<-------- Address/Data 4
$\overline{RD}$ ---------->	F	6	<-------- Address/Data 5
Timer One Input ----->	H	7	<-------- Address/Data 6
$\overline{PSEN}$ ---------->	J	8	<-------- Address/Data 7
Timer Two Input ----->	K	9	<-------- Address/Data 0
Timer Two Trigger --->	L	10	<------- Address/Data 1
TTL Serial Out ------>	M	11	<------- Address/Data 2
TTL Serial In ------->	N	12	<------- Pulse Width Mod.
$\overline{\text{Int 0 - DMA Req}}$ ---->	P	13	<------- $\overline{\text{Interrupt 1}}$
$\overline{\text{DMA Acknowledge}}$ ---->	R	14	<------- $\overline{\text{Program Enable}}$
Address 15 ---------->	S	15	<------- $\overline{\text{Program Pulse}}$
Address 14 ---------->	T	16	<------- No Connection
Address 13 ---------->	U	17	<------- No Connection
Address 12 ---------->	V	18	<------- No Connection
Address 11 ---------->	W	19	<------- No Connection
Address 10 ---------->	X	20	<------- RD/$\overline{WR}$
Address 9 ----------->	Y	21	<------- $\overline{DS}$
Address 8 ----------->	Z	22	<------- $\overline{AS}$

FIG. 26

LCD DRIVER (BCC25) PIN CONNECT TO

MMZ8 Bus Pin Configuration
End View - Edge Card Connector
(signals not used on this board are in parentheses)

(- 12 Volts)	A	[	]	1	+ 5 Volts
(+ 12 Volts)	B	[	]	2	Ground
Reset	C	[	]	3	(No Connection)
(No Connection)	D	[	]	4	Address/Data 3
(Timer 0 Input)	E	[	]	5	Address/Data 4
$\overline{RD}$	F	[	]	6	Address/Data 5
(Timer 1 Input)	H	[	]	7	Address/Data 6
$\overline{PSEN}$	J	[	]	8	Address/Data 7
(Timer 2 Input)	K	[	]	9	Address/Data 0
(Timer 2 Trigger)	L	[	]	10	Address/Data 1
(TTL Serial Output) -	M	[	]	11	Address/Data 2
(TTL Serial Input)	N	[	]	12	(PW Modulator)
$\overline{\text{Int 0 - DMA Request}}$	P	[	]	13	$\overline{\text{Int 1}}$
$\overline{\text{(DMA Acknowledge)}}$	R	[	]	14	$\overline{\text{(Prog Enable)}}$
Address 15	S	[	]	15	$\overline{\text{(Program Pulse)}}$
Address 14	T	[	]	16	(No Connection)
Address 13	U	[	]	17	(No Connection)
Address 12	V	[	]	18	(No Connection)
Address 11	W	[	]	19	(No Connection)
Address 10	X	[	]	20	RD/$\overline{WR}$
Address 9	Y	[	]	21	$\overline{DS}$
Address 8	Z	[	]	22	$\overline{AS}$

FIG. 26A

J1

Console Serial Connector
(DB-25S RS-232 Connector - Top View)

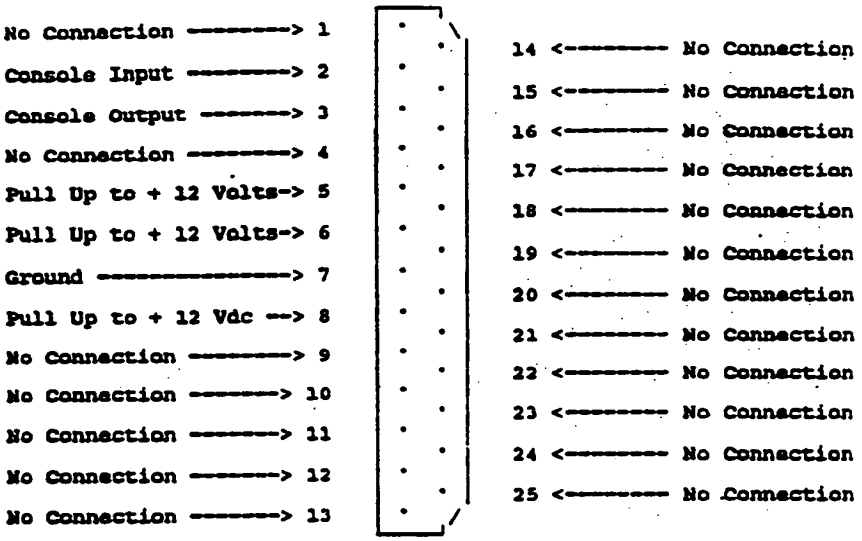


FIG. 27

J2

Serial Printer Connector
(2 X 10 Pin Berg Header - Top View)

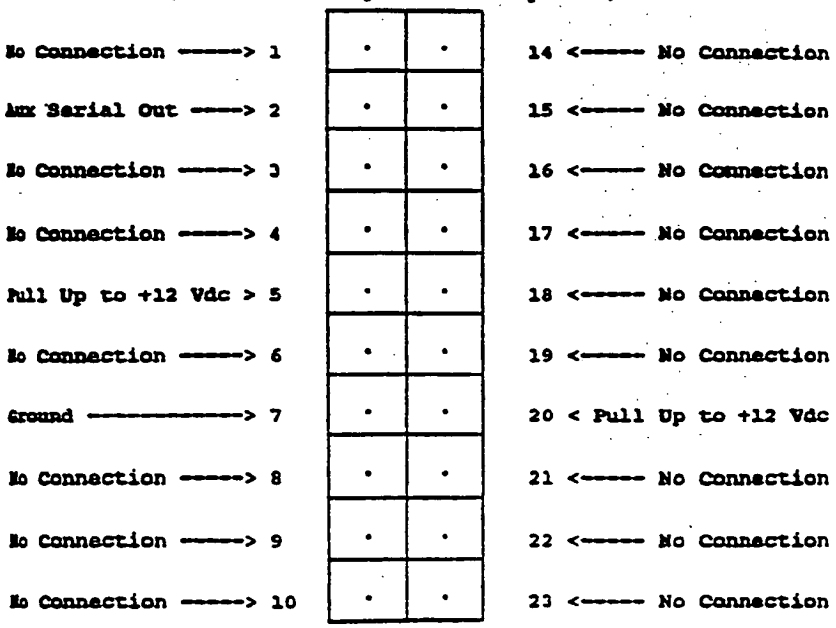


FIG. 28

FIG. 29

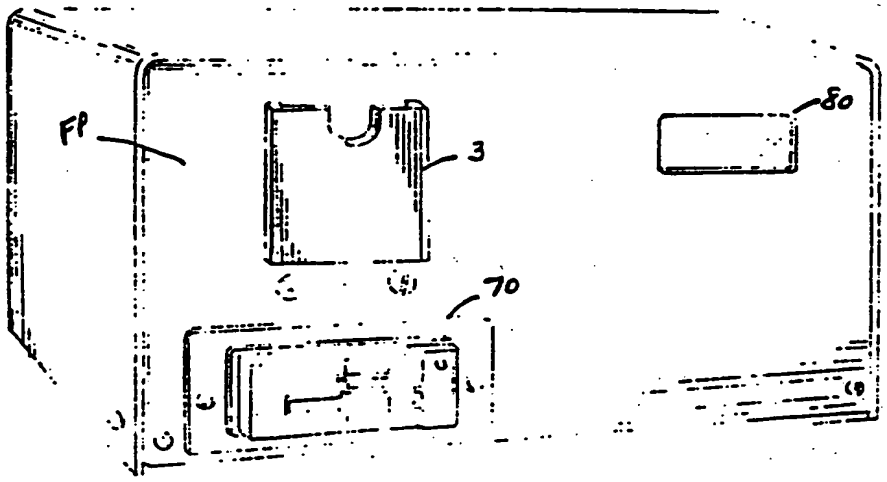


FIG. 30

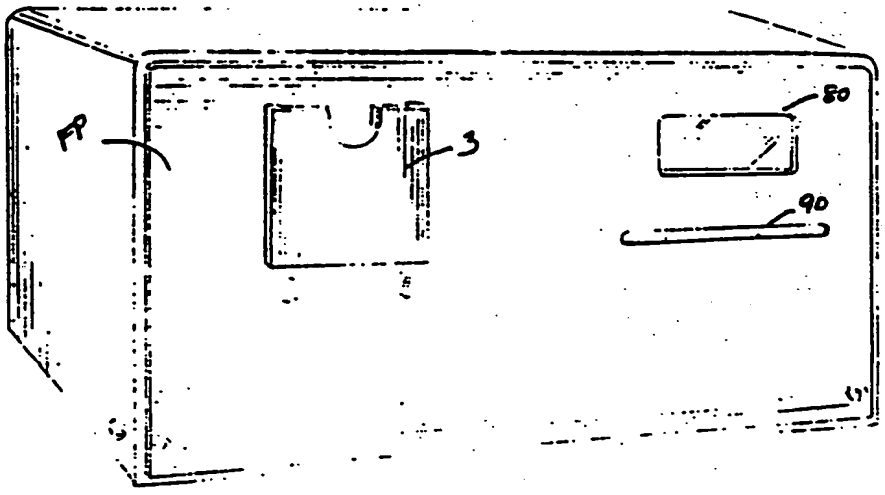
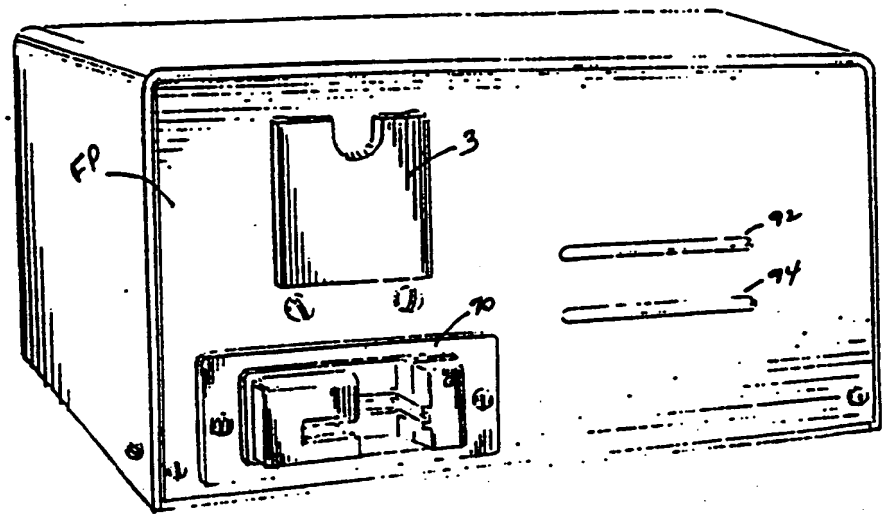


FIG. 31



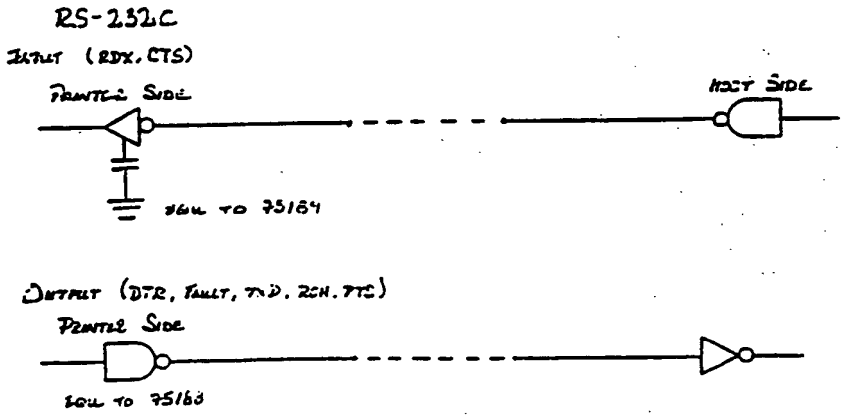


FIGURE. 32 PRINTER INTERFACE

FIG. 33

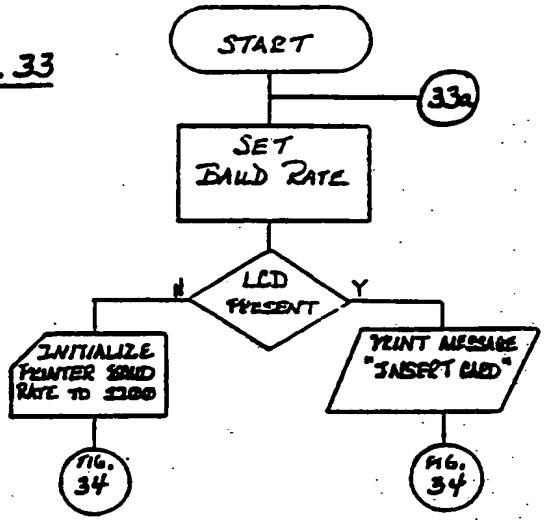
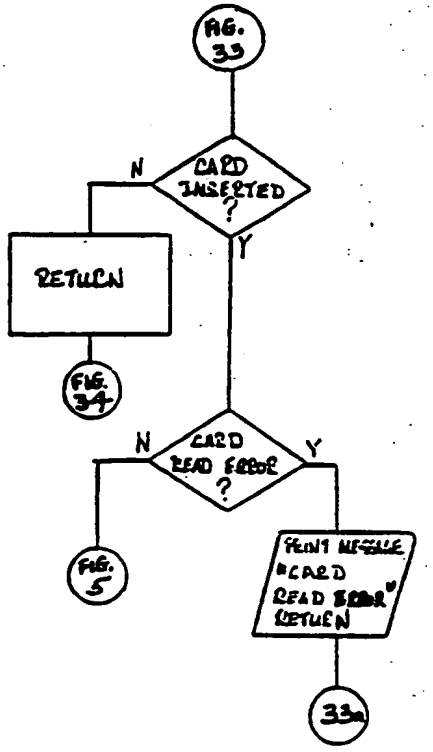


FIGURE 34



INTERNATIONAL SEARCH REPORT

International Application No PCT/US90/06172

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [3]

According to International Patent Classification (IPC) or to both National Classification and IPC

INT. CL.(5): G06K 9/00
US CL.: 382/5

II. FIELDS SEARCHED

Minimum Documentation Searched [4]

Classification System	Classification Symbols
U.S.	382/1,2,4,5 340/825.34

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [5]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [14]

Category *	Citation of Document, [16] with indication, where appropriate, of the relevant passages [17]	Relevant to Claim No. [18]
X Y	US, A, 4,747,147 (SPARROW) 24 May 1988, See Figs. 1A-C, 4, 5b and column 3, line 55 through column 6, line 16.	1-4,6,8,64,65,121 141-146,148-150, 157/5,7,9,66,147
X Y	US, A, 4,896,363 (TAYLOR ET AL.) 23 January 1990, See Figs. 1-2 and column 4, line 65 through column 7, line 47.	1-4,6,8,64,65,121 141-146,148-150, 157/5,7,9,66,147
X Y	US, A, 4,944,021 (HOSHINO ET AL.) 24 July 1990, See Figs. 1-3 and 6-9 and refer to column 2, line 35 through column 7, line 4.	141-146,148-150, 157/1-9,64-66, 121-147
Y	US, A, 4,811.414 (FISHBINE ET AL.) 07 March 1989, See Figs. 1-47 and column 6, line 9 through column 9, line 37.	1-9,64-66,121, 141-150,157
Y	US, A, 4,210,899 (SWONGER ET AL.) 01 July 1980, See Figs. 1-4 and column 3, line 46 to column 6, line 4.	1-9,64-66,121, 141-150,157

* Special categories of cited documents: [13]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search [2]	Date of Mailing of this International Search Report [9]
11 FEBRUARY 1991	01 APR 1991
International Searching Authority [1]	**Signature of Authorized Officer** [20]
ISA/US	JOSE L. COUSO

Form PCT/ISA/210 (second sheet) (May 1986)

FURTHER INFORMATION CONTINUED FROM THE SECOND SHEET

V. ☐ OBSERVATIONS WHERE CERTAIN CLAIMS WERE FOUND UNSEARCHABLE [1]

This international search report has not been established in respect of certain claims under Article 17(2) (a) for the following reasons:

1. ☐ Claim numbers . because they relate to subject matter [1] not required to be searched by this Authority, namely:

2. ☐ Claim numbers . because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out [1], specifically:

3. ☐ Claim numbers_____, because they are dependent claims not drafted in accordance with the second and third sentences of PCT Rule 6.4(a).

VI. ☒ OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING [2]

This International Searching Authority found multiple inventions in this international application as follows:

See Attached Sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims of the international application.

2. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims of the international application for which fees were paid, specifically claims:

3. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claim numbers:

1-9,64-66,121

4. ☐ 141-150,157 As all searchable claims could be searched without effort justifying an additional fee, the International Searching Authority did not invite payment of any additional fee.

Remark on Protest

☐ The additional search fees were accompanied by applicant's protest.

☐ No protest accompanied the payment of additional search fees.

IV. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING

Invention I Claims 1-9,64-66,121
Invention II Claims 10-18,67-69,123
Invention III Claims 28-40,70,117,118
Invention IV Claims 50-63,71,119,120

Invention VII Claims 76-77,122,124
Invention VIII Claims 104-114
Invention IX Claims 125-130,137,138
Invention X Claims 131-136,139,140

Invention V Claims 19-17
Invention VI Claims 41-49
Invention XI Claims 72-80
Invention XII Claims 81-94
Invention XIII Claims 141-150,157
Invention XIV Claims 151-153,156
Invention XV Claims 154-155

US, A,817,183 published 28 March 1989, See Figures 1A-4.

Groups I and XIII were examined, since group I was the first mention invention and form 206 indicated that group XIII would be examined without any additional fees being paid.